2019

Transparent User Authentication For Mobile Applications

Alotaibi, Saud Nejr S

UNIVERSITY OF
PLYMOUTH

Transparent User Authentication for Mobile Applications

By

Saud Nejr S Alotaibi

A thesis submitted to the University of Plymouth in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics

May 2019

Abstract

Transparent User Authentication for Mobile Applications

Saud Nejr S Alotaibi

The use of smartphones in our daily lives has grown steadily, due to the combination of mobility and round-the-clock multi-connectivity. In particular, smartphones are used to perform activities, such as sending emails, transferring money via mobile Internet banking, making calls, texting, surfing the Internet, viewing documents, storing medical, confidential and personal information, shopping online and playing games. Some active applications are considered sensitive and confidential and the risks are high in the event of the loss of any sensitive data or privacy breaches. In addition, after the point of entry, using techniques such as a PIN or password, the user of the device can perform almost all tasks, of different risk levels, without having to re-authenticate periodically to re-validate the user's identity. Furthermore, the current point-of-entry authentication mechanisms consider all the applications on a mobile device to have the same level of importance and so do not apply any further access control rules. As a result, with the rapid growth of smartphones for use in daily life, securing the sensitive data stored upon them makes authentication of paramount importance.

In this research, it is argued that within a single mobile application there are different processes operating on the same data but with differing risks attached. The unauthorised disclosure or modification of mobile data has the potential to lead to a number of undesirable consequences for the user. Thus, there is no

single level of risk associated with a given application and the risk level changes during use. In this context, a novel mobile applications data risk assessment model is proposed to appreciate the risk involved within an application (intra-process security). Accordingly, there is a need to suggest a method to be applied continuously and transparently (i.e., without obstructing the user's activities) to authenticate legitimate users, which is maintained beyond point of entry, without the explicit involvement of the user. To this end, a transparent and continuous authentication mechanism provides a basis for convenient and secure re-authentication of the user. The mechanism is used to gather user data in the background without requiring any dedicated activity, by regularly and periodically checking user behaviour to provide continuous monitoring for the protection of the smartphone.

In order to investigate the feasibility of the proposed system, a study involving data collected from 76 participants over a one-month period using 12 mobile applications was undertaken. A series of four experiments were conducted based upon data from one month of normal device usage. The first experiment sought to explore the intra-process (i.e., within-app) and inter-process (i.e., access-only app) access levels across different time windows. The experimental results show that this approach achieved desirable outcomes for applying a transparent authentication system at an intra-process level, with an average of 6% intrusive authentication requests. Having achieved promising experimental results, it was identified that there were some users who undertook an insufficient number of activities on the device and, therefore, achieved a high level of intrusive authentication requests. As a result, there was a need to investigate whether a specific combination of time windows would perform better with a specific type of user. To do this, the numbers of intrusive authentication requests were computed

based on three usage levels (high, medium and low) at both the intra- and inter-process access levels. This approach achieved better results when compared with the first set of results: the average percentage of intrusive authentication requests was 3%, which indicates a clear enhancement. The second and third experiments investigated only the intra-process and inter-process, respectively, to examine the effect of the access level. Finally, the fourth experiment investigated the impact of specific biometric modalities on overall system performance. In this research study, a Non-Intrusive Continuous Authentication (NICA) framework was applied by utilising two security mechanisms: Alert Level (AL) and Integrity Level (IL). During specific time windows, the AL process is used to seek valid samples. If there are no samples, the identity confidence is periodically reduced by a degradation function, which is 10% of current confidence in order to save power while the mobile device is inactive. In the case of the mobile user requesting to perform a task, the IL is applied to check the legitimacy of that user. If the identity confidence level is equal to or greater than the specified risk action level, transparent access is allowed. Otherwise, an intrusive authentication request is required in order to proceed with the service.

In summary, the experimental results show that this approach achieved sufficiently high results to fulfil the security obligations. The shortest time window of AL= 2 min / IL = 5 min produced an average intrusive authentication request rate of 18%, whereas the largest time window (AL= 20 min / IL = 20 min) provided 6%. Interestingly, when the participants were divided into three levels of usage, the average intrusive authentication request rate was 12% and 3% for the shortest time window (AL = 2 min / IL = 5 min) and the largest time window (AL= 20 min / IL = 20), respectively. Therefore, this approach has been demonstrated

to provide transparent and continuous protection to ensure the validity of the current user by understanding the risk involved within a given application.

Table of Contents

List of Figures

List of Tables

Glossary of Abbreviations

App	-	Application
ADB	-	Android Debug Bridge
AL	-	Alert Level
CCTA	-	Central Computer and Telecommunications Agency
CSCAN	-	Centre for Security, Communications and Network Research
CRAMM	-	CCTA Risk Analysis and Management Method
EER	-	Equal error rate
FAR	-	False acceptance rate
FAST	-	Finger Gestures Authentication System
FRR	-	False rejection rate
IAMS	-	Intelligent Authentication Management System
IBG	-	International Biometrics Group
IL	-	Integrity Level
MASP	-	Managed Authentication Service Provider
MORI	-	Mobile Risk
NICA	-	Non-Intrusive Continuous Authentication
OS	-	Operating system
OTP	-	One-time password
PIN	-	Personal identification number
RFID	-	Radio-frequency identification
TAR	-	True acceptance rate
TAS	-	Transparent authentication system
TRR	-	True rejection rate

Acknowledgements

First and foremost, all praise and gratitude are due to Allah Almighty, the All Merciful, for helping me and facilitating me in tackling all the challenges throughout this PhD which could have constrained my study.

I am deeply indebted and most of my sincere thanks and appreciation go to my beloved parents, for their considerable help and support, kindness, abundant love, and prayers for my study and I ask Allah to reward them with the best. I would also like to take this opportunity to express my sincere gratitude to my brothers and sisters for their immeasurable love and encouragement through this important stage of my life; my sincere appreciation goes to the soul of my little brothers, Diaffallah and Mohammed (may Allah have mercy upon them). For my parents, brothers and sisters, I am forever grateful.

I also owe many thanks to my wives and my children, Zeyad, Reema, Yasir, and Omar, for their patience, endless support, and incredible care in assisting me throughout this endeavour. They all stood alongside me and provided me with an abundance of love and support, even when spending days, nights, and holidays without me. I really appreciate your endless support and help through this PhD journey. I am eternally grateful.

Of course, I would like to extend my most sincere thanks and my heartfelt appreciation to my supervision team, Professor Steven Furnell and Professor Nathan Clarke, for their guidance, support, wisdom, help and a sympathetic ear. Their experience and professionalism in various aspects, such as their critical thinking, publications and presentations, have been invaluable throughout my PhD journey and without their valuable comments and advice, I would not be able to make this a success, so thank you.

I would also like to express my thanks to my research colleagues at the Centre for Security, Communication and Network Research, Abdulrahman Alruban and Abdulwahid Al Abdulwahid, who have been my motivation and inspiration and with whom I have held interesting discussions during this PhD journey; and to Yaseen Salem, who was the first participant in my data collection, and to all the participants who contributed their mobile user interactions to this research project; without them, this research study would have been impossible.

I would like to take this opportunity to thank all my colleagues at the Ministry of the Interior in the Kingdom of Saudi Arabia for allowing me to take this great opportunity to complete my PhD degree and for their support and assistance. In particular, special thanks go to the former directors of the Information Technology Department, namely, Engineer Abdullah Abo Deraa, Colonel Mohammed Alqahtany, Najee Alqahtany and Major Khaled Al Mohammedi. Special thanks must also go to my colleagues in the Ghazalah group, for being wonderful friends and for their sincere suggestions and continuous encouragement.

Last, but not least, many thanks and much appreciation must go to my Government of The Custodian of the Two Holy Mosques and the Minister of the Interior for sponsoring my undertaking of the research project and for their generous support and valuable comments.

I dedicate this to my children: Zeyad, Reema, Yasir, and Omar.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Doctoral College Quality Sub-Committee.

Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

This study was financed with the aid of a scholarship from the Kingdom of Saudi Arabia - Royal Embassy of Saudi Arabia Cultural Bureau in London.

Publications:

•Alotaibi, S., Furnell, S., and Clarke, N. (2016). MORI: An Innovative Mobile Applications Data Risk Assessment Model. In the Journal of Internet Technology and Secured Transactions (JITST), Vol. 5, Iss. 3/4, September/December 2016. DOI: 10.20533/jitst.2046.3723.2016.0062

•Alotaibi, S., Furnell S., and Clarke N., (2016). A Novel Taxonomy for Mobile Applications Data. In the International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol. 5, No. 3, pp. 115-121. (ISSN: 2305-0012)

•Alotaibi, S., Furnell, S., and Clarke, N. (2018). A Novel Transparent User Authentication Approach for Mobile Applications. Information Security Journal: a Global Perspective. DOI: https://doi.org/10.1080/19393555.2019.1609628

Presentations at conferences:

•Alotaibi, S., Furnell, S., and Clarke, N. (2015, December). Transparent authentication systems for mobile device security: A review. In Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for (pp. 406-413). IEEE. London, UK. DOI: 10.1109/ICITST.2015.7412131

Word count of thesis: 42,561

Signed _____Saud_____

Date_____15/04/2019_____

Chapter One

Introduction

1 Introduction

1.1 Introduction

Mobile phones are used to perform activities such as sending emails, transferring money via mobile Internet banking, making calls, texting, surfing the Internet, viewing documents, storing medical, confidential and personal information, shopping online and playing games. Some of these active applications are considered sensitive and confidential and are becoming an ever more pressing concern, as the risks are high for users in the event of the loss of sensitive data or a privacy breach (Tam et al., 2015; Patel et al., 2016). In addition, with the rapid growth of mobile devices for use in our daily life, securing the sensitive data stored upon them makes authentication of paramount importance. Interestingly, 36% of mobile phone users have reported not safeguarding their mobile phones by applying a personal identification number (PIN) or password approach (Siciliano, 2013) and 44% of the surveyed respondents changed their password only once a year or less (CSID, 2012). Furthermore, Gartner (2013) forecasted that, in 2017, the main breaches would be of mobile devices and tablets. In particular, mobile application misconfigurations would be the most common, accounting for approximately 75% of all mobile security breaches.

Furthermore, after the point-of-entry authentication stage at the beginning of a session, by using a PIN or password, the user of the device can perform almost all tasks, regardless of the different risk levels, without periodically having to re-authenticate to re-validate the user's identity. Current point-of-entry authentication mechanisms also consider all applications on the mobile device to have the same level of importance and keep a single level of security for all applications, thereby not applying any further access control rules (Clarke et al., 2009). As a result, it is argued that different

applications require different security provision; for instance, a bank account requires a different level of protection compared with a short message service (SMS) message. Consequently, each application has a particular level of risk which might be a feature that defines a suitable level of security (Ledermuller and Clarke, 2011). In their research, it is argued that, on a single mobile application, different processes operate on the same data with a different social risk based on the user action. More specifically, the unauthorised disclosure or modification of mobile applications data has the potential to lead to a number of undesirable consequences for the user. Thus, there is no single category of risk in using a single application; applications have a different level of risk that changes within the application.

Accordingly, there is a need to suggest a method that could be applied continuously and transparently, without obstructing users' activities, to authenticate legitimate users, which is maintained beyond the point of entry, without the explicit involvement of the user. To this end, a transparent and continuous authentication mechanism would provide a basis for the convenient and secure re-authentication of the user and thereby gather user data in the background without requiring any dedicated activity (Clarke et al., 2009; Chuang et al., 2018), by regularly and periodically checking user behaviour to enable the continuous monitoring of the protection of the mobile device.

To conclude, this research project mainly investigates the following research question:

> *Are we able to apply transparent authentication systems based on the risk level by utilising a combination of the device owner's biometrics?*

Two tasks were undertaken to address the above research question fully: firstly, an investigation of the risk level for each service within a given application was conducted by classifying the mobile application's data and then suggesting a risk matrix to calculate the risk level for each service; and secondly, the impact of the inter- and intra-

processes on the overall transparent user authentication approach for mobile applications was tested through a series of experimental analysis studies. These experiments aimed to compute the total number of intrusive user authentication requests by collecting log data from a total of 76 participants over one month of normal device usage.

To test the concept, the proposed framework is based on Clarke and Furnell (2007) and adjusted the biometric modalities, feature extraction, authentication manager and intrusive algorithm, as shown in Figure 1-1. The proposed framework consists of a number of key components, including a Data Collection Engine, a Biometric Profile Engine, and an Authentication Engine. These engines perform various tasks, such as collecting biometric data, generating user profiles, and verifying a user's identity, respectively. There are two further main system components: the Authentication Manager, which controls the three previously mentioned engines; and the Intra-Process Determination System, which observes the user action on a specific application.

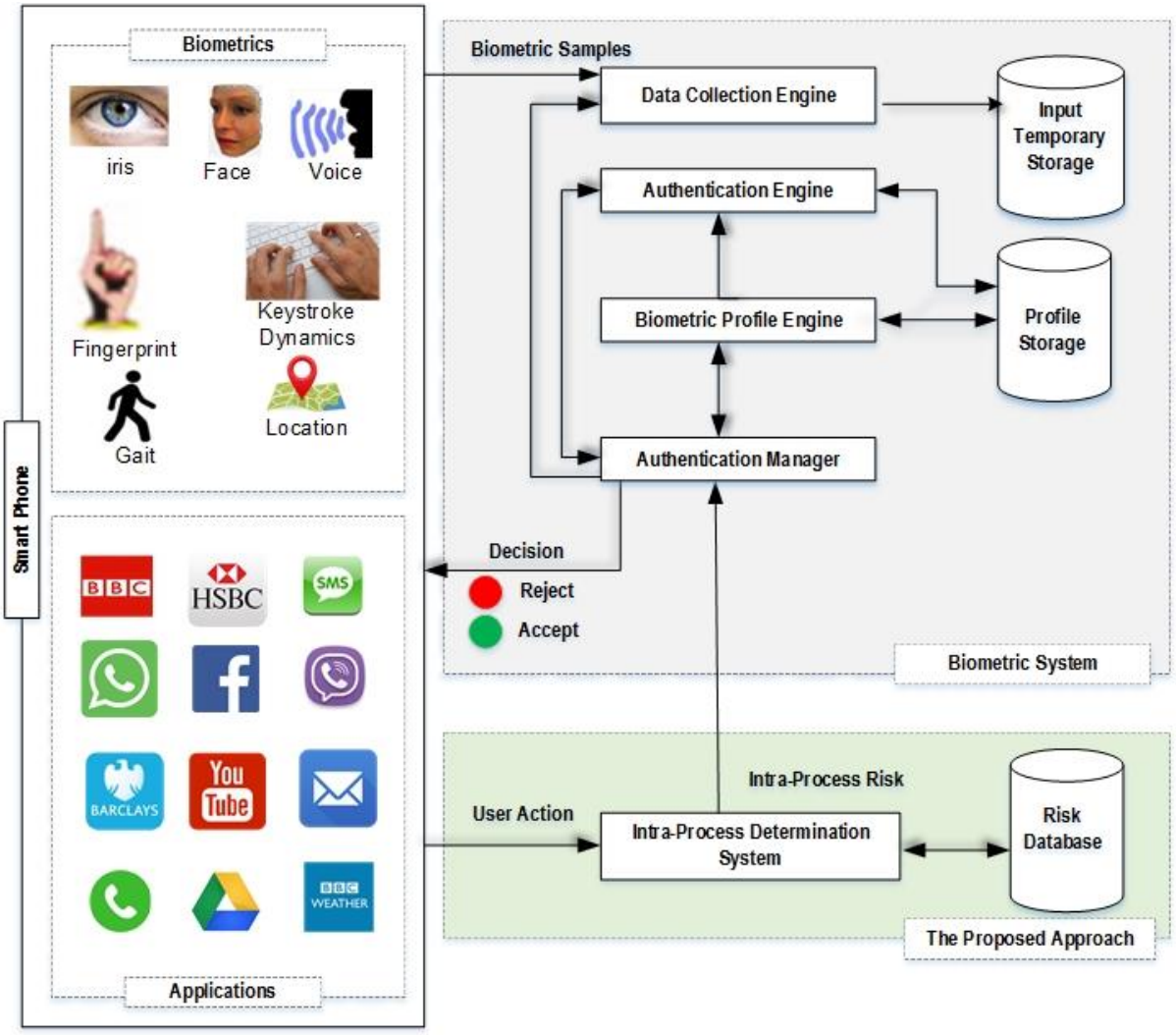


Figure 1-1: Framework for mobile application security (based on Clarke et al, 2009)

- **Authentication Manager**: The main functionality of the Authentication Manager is to observe the current security level and make authentication decisions if the user requests access to a service within the application (intra-process). For the purpose of checking whether the user is allowed to access this service within the application, the Authentication Manager compares the risk level value for this intra-process, which is retrieved from the Risk Database, with the confidence level value calculated by the Authentication Engine. If the process risk value exceeds the threshold (confidence level), the user will be allowed access. Otherwise, if the process risk value is less than the threshold, the user

will be denied access to the service. In this context, the risk level value will be one of the following: no risk, low risk, medium risk, and high risk, each of which has a predefined value.

- **User Action Determination System (new component)**: The previous stage (i.e. Authentication Manager) involved collecting real biometric sample data from the user and comparing them with a biometric template in order to generate a confidence level. Then, this value is passed to the Authentication Manager for comparison with the risk value for the process. The risk value is based on this new component. The novel elements are the ability to determine and identify the current user's action on the application (intra-process), which is the key task of the Intra-Process Determination system. The outputs from this component are an application name and the intra-process name within this application, both of which will be sent to the Authentication Manager in order to decide the legitimacy of the user and whether the action can be accomplished. Figure 1-1 demonstrates the framework architecture for the intra-process security system.

1.2 Aims and Objectives

The aim of this research is to *propose and develop an intelligent transparent authentication framework for the intra-process security of mobile applications that fulfils the security obligations and provides continuous protection to ensure the validity of the current user.* In order to achieve this aim, the research project is divided into five distinct objectives:

- **Objective 1**: To produce a novel mobile applications data taxonomy by investigating the risk for each process within an application in order to explore user action risk.

- **Objective 2**: To propose an innovative risk assessment model for mobile applications data, called MORI (Mobile Risk), which can be used to determine the risk level for each action on a single application.
- **Objective 3**: To develop user action determination software in order to create a real dataset to utilise in the study experiments.
- **Objective 4**: Investigating the potential for applying a transparent authentication system to intra-process security for mobile applications by conducting a series of experiments.
- **Objective 5**: To investigate the impact of specific biometric modalities on the overall system performance in three types of modality: single, two, and multi modalities.

1.3 Novel Research Contributions

This research is suitable for mobile application developers due to there is a clear need to ensure the validity of the current user and provides continuous protection after the point of entry authentication phase. Likewise, this approach would achieve good levels of usability by utilizing a combination of the device owner's biometrics in the background without being prompted to authenticate again and without interrupting the user from their typical interaction with the mobile.

The research programme has accomplished the aforementioned objectives, contributed new knowledge and improved the field of user authentication for smartphones in general and mobile application security and usability in particular.

The key novel contributions of this research project are briefly listed below:

- Producing comprehensive analysis and a systematic literature review of transparent authentication systems for mobile device security which indicate

there is a clear need to investigate when to authenticate a mobile user by focusing on the sensitivity level of the application and understanding whether a certain application may require protection.

- Drawing attention to studying the risk for each process within an application and introducing a novel taxonomy of mobile applications data by studying the risk for each process within the given application.
- Introducing a new risk assessment model for mobile applications data, called MORI (Mobile Risk), which determines the risk level for each process on a single application. The risk matrix could, in future, assist research activities that investigate the risks within an application and might help to move the access control system from the application level to the intra-process application level, based on the level of risk of the user action being performed.
- Conducting a set of experiments aimed at better understanding and investigating the potential for applying a transparent authentication system to intra-process security for mobile applications.
- Studying the impact of each individual modality on overall system performance by creating a series of experiments to investigate this.

A number of scientific papers relevant to this research project have been published and presented in refereed journals and conferences and several papers have been prepared for publication. The outcomes of this research study are listed below:

Alotaibi, S., Furnell, S., & Clarke, N. (2015, December). Transparent authentication systems for mobile device security: A review. In Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for (pp. 406-413). IEEE. London, UK.

Alotaibi, S., Furnell S., and Clarke N., (2016). A Novel Taxonomy for Mobile Applications Data. In the International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol. 5, No. 3, pp. 115-121.

Alotaibi, S., Furnell, S., & Clarke, N. (2016). MORI: An Innovative Mobile Applications Data Risk Assessment Model. In the Journal of Internet Technology and Secured Transactions (JITST), Vol. 5, Iss. 3/4, September/December 2016.

Alotaibi, S., Furnell, S., & Clarke, N. (2018). A Novel Transparent User Authentication Approach for Mobile Applications. Submitted to Information Security Journal: a Global Perspective.

1.4 Thesis Structure

This research project is organised into seven chapters in order to present the achievements relating to the above-mentioned objectives. The first chapter identifies the research problem and highlights the research study aim and objectives, its novel research contributions and, finally, the structure of the thesis.

The second chapter, *mobile device authentication*, provides background information about mobile and biometric authentication. Firstly, it reviews the popularity of mobile devices, the increasing reliance upon them and establishes the importance of security for these devices. The chapter continues by providing an overview of some of the currently provided authentication technologies and reviews biometric authentication from a number of perspectives, including its system components, requirements, techniques, performance measures and fusion. The chapter ends with an account of the current authentication mechanisms for mobile devices.

The third chapter, *a systemic review of continuous and transparent authentication systems for mobile devices*, briefly outlines the concept of a transparent authentication system and why it is needed. This is followed by a literature review of the existing research in this domain on continuous and transparent authentication systems for mobile devices and provides a comparative summary of each category. The chapter concludes with a discussion and identifies a gap that exists in the literature by highlighting the need for a new security mechanism that can provide continuous and transparent protection for mobile devices.

The fourth chapter *introduces a novel mobile applications data risk assessment model*. The chapter explains the need for intra-process security for mobile devices through examples of different types of applications. Then, a taxonomy of mobile applications data is presented, with justifications. Finally, the chapter presents a generic risk assessment model for mobile applications data with a particular focus on analysing and producing a risk matrix.

The fifth chapter, *a transparent, intra-process user authentication approach for mobile applications*, presents the experimental methodologies, analysis and results regarding the novelty of the proposed model. After presenting the data collection methodology and the software generated to collect user interactions with a smartphone in a real data environment, three types of experiment are presented in great detail. The first experiment sought to explore the intra-process (i.e., within-app) and inter-process (i.e., only-app) access levels across different time windows and achieved promising experimental results when the 76 participants were also classified into three groups according to their level of mobile usage. The second experiment was conducted to provide further insight into whether applying a transparent authentication system to the intra-process only would enhance security and usability. Finally, to prove the research

concept, it was deemed useful to conduct an evaluation using the same real-world dataset. To achieve this goal, the average intrusive authentication requests were calculated and presented for the inter-process (application access only) without taking the actions that happened within an application into account. This is followed by a table summary of all the experiments with more detail and discussion.

The sixth chapter, *investigating the impact of each simulated modality on the overall system performance*, seeks to test the effect of biometrics on the system results. This investigation conducted three types of experiment employed without the selected modality, calculated the total intrusive authentication requests and compared these with the overall system performance. The chapter then presents examples of different participants in each experiment.

The seventh chapter, *conclusions and future work*, is the final chapter and highlights the main contributions and achievements of this research project in relation to the field of user authentication for smartphones in general and mobile applications security and usability in particular. The limitations of the research project, suggestions and scope for future work, and the future for user authentication on mobile devices are explored and discussed at the end of the chapter.

At the end of this thesis report, there are a number of appendices that support the main aim of this research project, such as confirmation of the ethical approval for the experiments, the consent forms given to the participants, programming scripts, and a series of peer-reviewed publications resulting from this research study.

Chapter Two

Mobile Device Authentication

2 Mobile Device Authentication

2.1 Importance of Mobile Devices

The use of mobile devices in our daily lives has grown steadily, due to the combination of mobility and 24/7 multi-connectivity (Spaccapetra et al., 2005). As a result, mobile devices have overtaken desktop computers (Miles, 2015). Figure 2-1 shows the total number of smartphone users worldwide from 2014 to projections for 2022. The number of smartphone users in 2019 is forecast to pass 5 billion. For example, in the USA, the number is forecast to grow to 247.5 million by 2019. In addition, 80% of Internet users own a smartphone (Smart Insights, 2015) and over 50% of smartphone users pick up their smartphone immediately after waking up (ExpressPigeon, 2014). Globally, there are 3.419 billion people connected to the Internet (equating to 46% global penetration), while 2.307 billion users are actively involved in social media. In addition, 3.790 billion people are unique mobile users (representing 51% global penetration), whereas 1.968 billion users utilise social media on a mobile device (we are social, 2016).

Furthermore, the size of the mobile market has increased significantly each year, while mobile phone users' subscriptions reached an estimated 7 billion by 2015, according to one report (ITU, 2015). Statistics also show the number of smartphone users in the UK from 2011 to 2014 and provide a forecast through 2018; the forecast estimated that the number of smartphone users would reach about 44.9 million by 2017 (Statista, 2016).

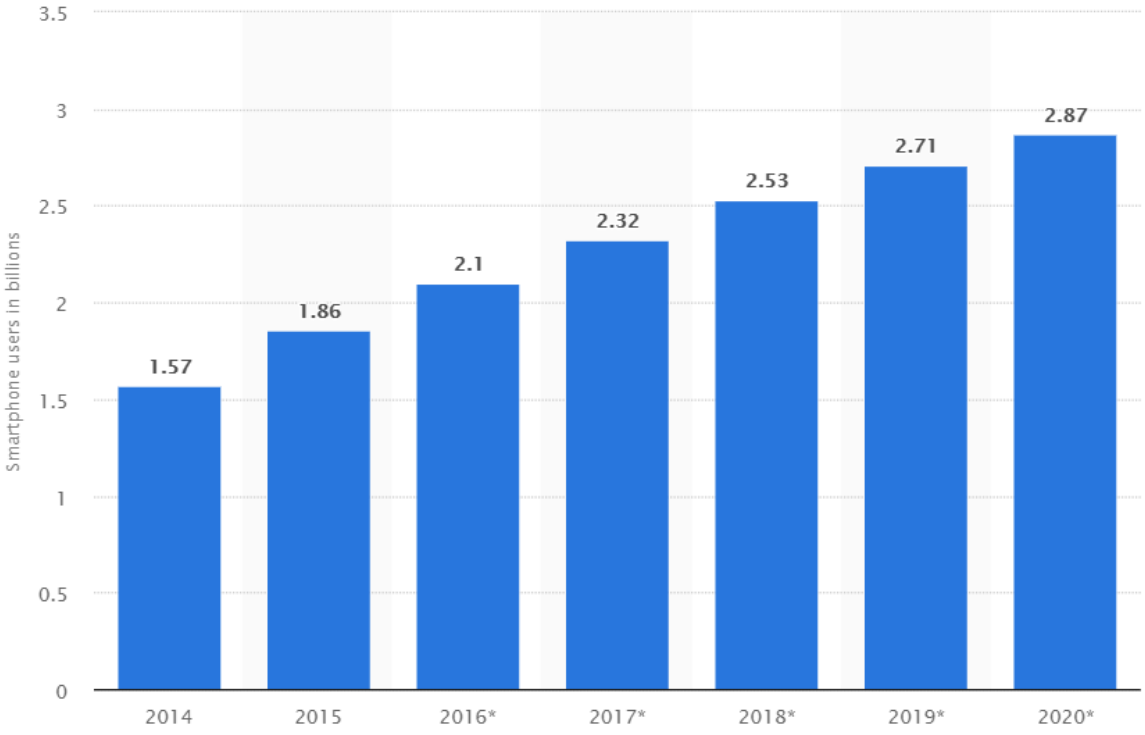


Figure 2-1: Number of smartphone users worldwide (Statista, 2018)

2.2 Mobile Applications Evolution

The global mobile applications market was forecast to reach $25 billion by the end of 2015 (ABI Research, 2010). Statista (2016 b) predicted that, in 2020, the expected growth of mobile app revenue would be $101 billion, from $41.1 billion in 2015. It was expected that revenue from mobile apps would grow at a steady rate in the coming years. Moreover, mobile web traffic was expected to exceed 10 exabyte by 2017 (Nicolaou, 2013). Regarding the digital marketing review (comScore, 2018), mobile devices achieve 75% of all adults' time online with smartphones. On the other hand, 80% of female spend their time on mobile devices compare with only 69% for males and 30% of online adults are now mobile only as well. Based on audience, over 90% of time online is spent on smartphones for Spotify and Snapchat whereas tablets account for over a third of time spent on the BBC as illustrated in Figure 2-2. In addition, YouTube increased both its mobile app audience (about 5%) and time spent

(about 22%) compared to 2017. Interestingly, Snap is the only mobile app in the top 10 which is not owned by Google or Facebook. Furthermore, Spotify, Netflix and eBay feature in the top 10 mobile apps for time spent (comscore, 2018).

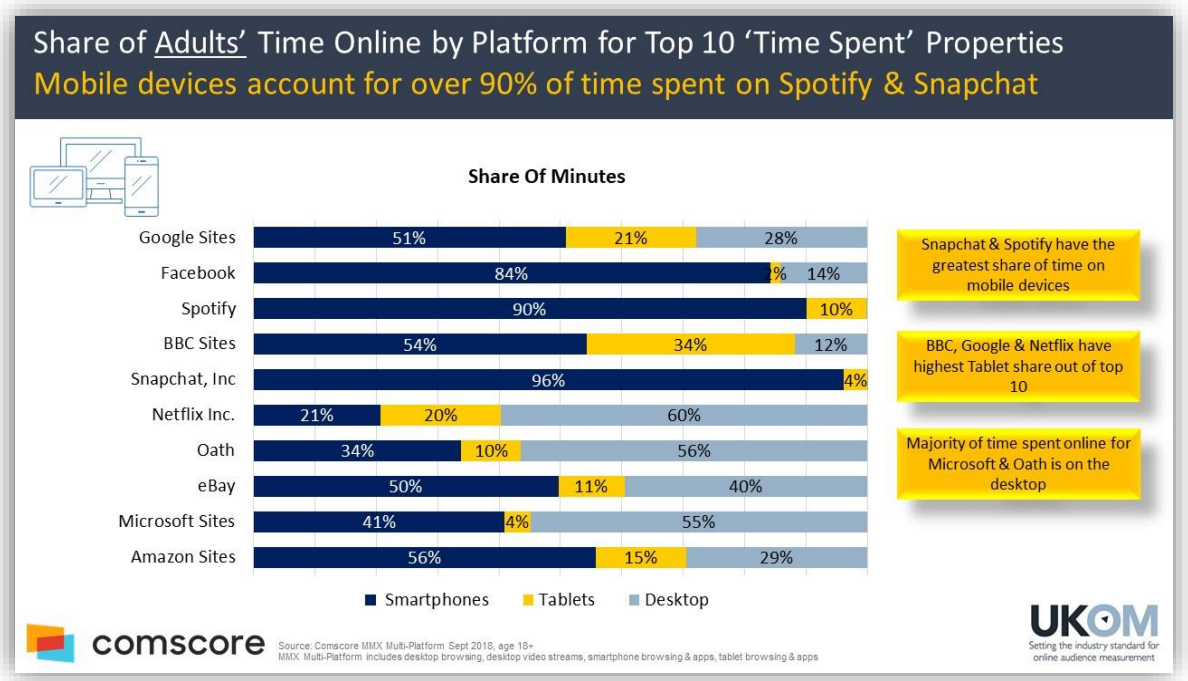


Figure 2-2: UK digital marketing review (comscore, 2018)

In this context, Android was the fastest-growing operating system (OS) in terms of popularity, as well as the most widespread mobile OS (IDC, 2014; Statista, 2016 e). Statista (2016c) shows the number of apps available in the Google Play Store (Android Market) from December 2009 to February 2016. The number of apps available in the Google Play Store exceeded 1 million in July 2013 and was recently placed at 2 million in February 2016. In comparison, the Apple App Store offers 1.4 million apps (Statista, 2015). Furthermore, Android and iOS devices accounted for 97.5% of global smartphone sales (Statista, 2016e), as shown in Figure 2-3, from just 38% in 2010 (Chrome Info Technologies, 2016). As a result, by 2017, 50% of online transactions were conducted by mobile app. There are approximately 1 billion Android-activated

devices (King, 2013) and more than 1 billion monthly-active Android users (Fiegerman, 2014).

In the UK, Statista (2016d) presented a forecast of the number of mobile app users from the third quarter of 2013 to the second quarter of 2016. By the second quarter of 2016, it was forecast that there would be 43.2 million mobile app users in the UK.

Figure 2-3: Android and iOS market share (Statista, 2016 e)

2.3 User Authentication Approaches

User authentication is a vital concept for achieving a high level of security in an information technology (IT) system to protect it from unauthorised user actions. ISO 27000 (2016) define the authentication as: “Authentication is a process that is used to confirm that a claimed characteristic of an entity is actually correct. To authenticate is to verify that a characteristic or attribute that appears to be true is in fact true”. In order to grant access to a certain system, user authentication is the first phase of the access

control process to decide whether access can be allowed. Traditionally, authentication could be achieved by utilising one or more of the three following approaches (Wood, 1977):

1. Something you know, such as a password, PIN, or answer to a challenged cognitive question. This approach is known as secret knowledge-based authentication.
2. Something you have, such as a Smart/ATM card, radio-frequency identification (RFID) chip, keyfob or hardware/software one-time password (OTP) token. This is known as token-based authentication.
3. Something you are, such as biometrics, including physiological, such as fingerprints, iris and retina scans and facial recognition, and behavioural (referred to as something you do), for instance, typing, voice, and device use patterns.

As secret knowledge can be easy to share and to guess, this type of authentication can be combined with token-based authentication to increase the security provided, known as “two-factor authentication”. On the other hand, while biometrics can be more difficult to mimic or forge compared with knowledge or tokens, they are computationally more difficult to process (Crawford et al., 2013). Biometrics can require more hardware than other methods, although behavioural biometrics often do not. Therefore, combining multiple authentication methods, a process known as “multi-factor authentication”, tends to provide a better authentication mechanism and thereby enhances system security, but also complicates the process of authentication.

Nowadays, a new technology has been emerged called blockchain. Blockchain is a sequence of blocks which holds a complete list of transaction records. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data

(Xiong et al, 2018). Although blockchain has been widely adopted in many applications, there is a lack of the mechanism of identity binding (Gao et al, 2018: Lu, Y. 2018). In addition, this study is focus on gathering user data in the background without requiring any dedicated activity, by regularly and periodically checking user behaviour to provide continuous monitoring for the protection of the smartphone.

2.4 Secret Knowledge-based Authentication

Knowledge-based authentication methods, such as passwords and PINs in particular, are the most widely used authentication techniques, due to being easy to implement and not requiring additional hardware, despite there being significant issues involved in their use (Crawford et al., 2013). In this method, the user has to remember a secret PIN or password, an answer to a predefined question, or images.

A PIN is considered the simplest knowledge-based authentication technique due to its ease of recall, its perceived convenience, and its inexpensive implementation. For this reason, it is commonly used for authenticating a user's access to a mobile device and is widely used for ATMs with credit cards as a two-factor authentication scheme, although PINs are easier to guess and steal. On the other hand, passwords contain numbers, letters, and symbols, which reduces the possibility of being breached. In practice, the use of a password demonstrates that the person knows the secret for accessing an account, but not that he/she is the rightful owner. In addition, because a PIN has the same characteristics as a password, it faces the same issues of spying, guessing, and eavesdropping (Verizon, 2012; Patel et al., 2016). Clarke and Furnell (2005) show that 45% of the participants in their survey never change their PIN. Moreover, 71% of the participants of another survey did not even use a PIN or any other authentication method to safeguard their mobile phone (Kurkovsky and Syta, 2010). For example, 61% of users have reported reusing the same password on

multiple websites and 44% change their password once a year (CSID, 2012). As a result of having to create passwords for multiple accounts, users tend to write them down and/or select weak passwords that may be more easily remembered (O'Gorman, 2003).

A cognitive knowledge question seeks to mitigate the load on users having to memorise passwords by deploying associative question(s). These questions usually concern personal information, such as date of birth, mother's maiden name, and favourite colour. However, there is still a need to recall answers and the possibility of using social engineering or conducting online searches in order to obtain a user's answers. Therefore, this method would not be dependable as a stand-alone authentication approach.

On the other hand, with the aim of improving the usability of knowledge-based methods, graphical passwords are used and suggested to be alternatives to PIN, (Gyorffy, Tappenden & Miller, 2011) and improve password usage and are likely to overcome memorability problems. Humans also find it easy to recognise images, even after a period of time (Chiasson et al., 2007). A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface Instead of remembering characters (Katsini et al, 2016). Graphical password authentication techniques may be classified into four main categories (khan et al, 2019):

- **Recognition-based system**: users are permitted to choose an image from a given set of images during authentication and compared with they select the images at the registration phase.

- **Pure-recall-based system**: users set an image of their own choice and then they have to reproduce the same image during authentication.
- **Cued-recall-based system**: This technique is the same as Pure-recall but the only difference is that during authentication it provides users with clues to get authenticated.
- **Hybrid system**: This technique is usually a combination of two methods to overcome the vulnerability of a single technique.

2.5 Token-based Authentication

Token-based authentication is based on the use of something you have, such as a Universal Serial Bus (USB) token device, smart card, ID card, driving licence, or active password-generating security token to prove identity or eligibility in order to access a system. The advantage of this approach is that, rather than depending on human memory, it relies mainly on carrying a token and proving its ownership as an essential part of the entire authentication process. Therefore, it overcomes some of the weaknesses of a secret knowledge-based approach. Token-based authentication can be classified based on external appearance and the need for additional devices into two types: Hardware Tokens (token-based OTP) and Software Tokens (tokenless) (Aloul et al., 2009). A Hardware Token is a single-token physical device created and delivered by the service provider, for instance, the HSBC Secure Key OTP token; whereas, with Software Tokens, there is no need to carry a device due to the service provider sending the OTP via SMS to the user's registered mobile phone and requiring the user to enter the password generated to access a service.

Although token-based authentication is difficult to duplicate and manipulate, it is more expensive to implement (Tanvi et al., 2011) and presents possible inconveniences for the user, such as the need for additional hardware readers and having to carry a token

around. Thus, the use of tokens does not solve the problems faced when using knowledge-based authentication because a USB token can be stolen or attacked. User convenience is an issue, particularly when users need to carry a variety of tokens for different accounts and services from various providers (Al Abdulwahid et al., 2013). Moreover, it is apparent that the cost of issuing, maintaining and recovering tokens is higher. In addition, time synchronisation between a token and a system might be difficult with time-synchronous tokens (Furnell et al., 2008), especially in out-of-coverage areas.

Unlike biometric-based Authentication, secret knowledge based are vulnerable to be sharable, forgotten, and easy to guess (Ratha et al, 2011). Furthermore, secret knowledge based becomes quite difficult to remember and manage a big number of different accounts. In addition, token are vulnerable to be shared, can be duplicated, lost or stolen. On the other hand, biometric-based authentication is a unique feature which cannot be stolen, difficult to duplicate and nearly impossible to share. In this research study, security and usability can be increased by using transparent authentication due to the mobile device having a great source of data in terms of user biometrics and due to the weaknesses of secret knowledge based and token as well (Mahfouz et al, 2017).

2.6 Biometric-based Authentication

Biometrics are defined by the International Biometrics Group (IBG) as “the automated use of physiological or behavioural characteristics to determine or verify identity” (IBG, 2010). Biometrics are used for two purposes (Jain et al., 2008):

- **Verification**: in this type, the system matches the captured biometric characteristics of the claimed person with the stored template of that person in

a database. Therefore, the verification process checks whether the newly acquired sample matches the original sample's template by performing a one-to-one comparison. In this way, the system either rejects or accepts the submitted claim of identity. The verification process answers the following question: does this identity belong to you?

- **Identification**: In this mode, the system will verify the user by capturing a sample from the user and matching it against all the biometric reference templates stored in a database of registered users. In the identification process, the user has no need to claim an identity and the system performs a one-to-many comparison. Finally, this system is looking to find an identity, rather than verify a claimed identity. The identification process answers the following question: whose identity is this?

2.6.1 Biometric System Requirements

Jain et al. (2004) have recommended that a biometric characteristic should meet the following criteria in order to be utilised for an authentication system:

- **Universality**: Every user should have the characteristic being used as a biometric. For example, the user needs to have fingers for the fingerprint technique to be used as a biometric identifier.
- **Uniqueness**: The selected characteristics of a biometric should be sufficiently different in order to discriminate between them.
- **Permanence**: The biometric characteristic should not change over time; for instance, a person's fingerprints tend not to change over time, whereas the way in which a person types tends to alter. As a result, "the more the frequent changing

of a biometric, the more the need to update the biometrics template and therefore the higher the cost of maintenance“ (Clarke, 2011).

- **Collectability**: The biometric samples should be easy to capture, such as face images using a normal camera and capturing voice samples during a telephone call. In contrast, the user has to position the eye to a special infrared camera for a much longer time to obtain an iris image, a method that is considered intrusive.
- **Performance**: The proposed system should meet the requirements of accuracy, speed of matching, robustness and scalability of technologies.
- **Acceptability**: This refers to the level to which users prefer and accept the use of biometrics as an authentication scheme in their lives, such as a fingerprint scan compared with an iris scan.
- **Circumvention**: This means that the system should be adequately robust and stand up against various techniques, such as sample forgery. For instance, an iris scan is almost impossible to imitate. On the other hand, a fingerprint scan system can be fooled using a fake finger, while it is difficult to fake a facial thermograph-based authentication system with a replicated face, as the system has the ability to detect whether the face is alive.

2.6.2 Generic Biometric System

A biometric system consists of five incorporated generic components, as depicted in Figure 2-4 (Clarke, 2011):

- **Capture component** (data collection): The main aim of this component is to capture (the acquisition process) a biometric sample from a user by utilising a specific sensor. For instance, a camera could be used for capturing images of a face for facial recognition.

- **Feature extraction component** (processing)**:** The main purpose of this component is to extract a set of unique biometric data, known as a feature vector, after the sample is acquired using a number of algorithms, depending upon the biometric technique, to generate the biometric template (reference).

- **Storage component** (template database): The main goal of this database is to store the extracted unique features (biometric template) from the previous step to be used as a reference template for future comparison in the matching process. In addition, the templates in the database can be updated over time.

- **Classification component** (matching): The main objective of this component is to compare the biometric sample template (capture) with the stored template (reference) using a matching algorithm to generate a level of similarity or a matching score. Accordingly, the higher the value of the matching score, the more likely it is that the two biometric measurements originate from the same person. This matching process is applied either in the verification or identification stage.

- **Decision component:** This is the final component of a biometric system. The main aim of this component is to enable a decision by comparing the matching score that is produced from a classification process with the set threshold. Accordingly, the decision threshold is designated to permit the user access to the system in the case of verification or to identify the identity in the case of identification.

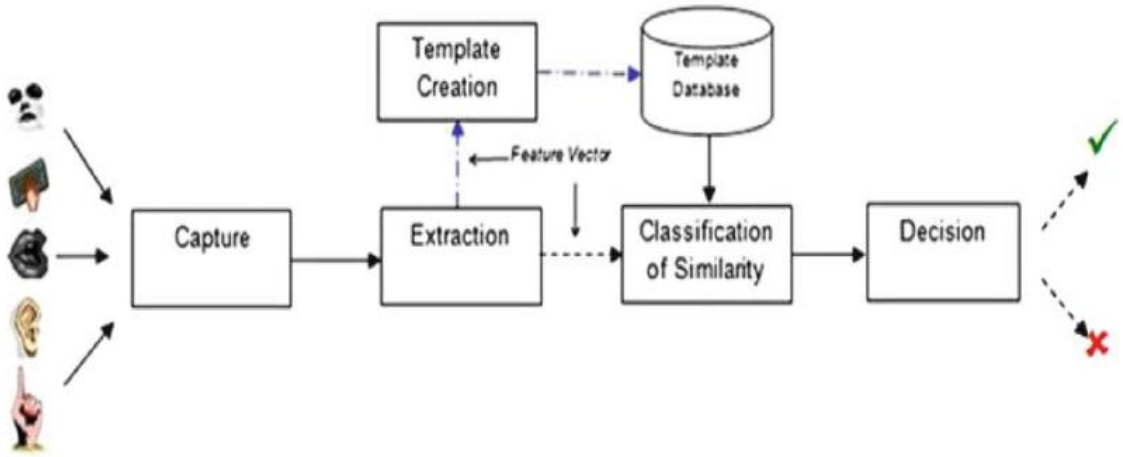


Figure 2-4: Components of a biometric system (Clarke, 2011)

In general, a biometric-based system consists of two stages: the enrolment process and the authentication process (Woodward et al., 2003; Jain et al., 2004), as shown in Figure 2-5.

- **Enrolment process** (registration): For the first step, an individual user needs to enrol on a biometric system. The user provides biometric information via a suitable sensor, then unique biometric characteristics are extracted, used to create a reference template, and stored in a database. The reference template is considered the main key to the success of a biometric system.

- **Authentication process** (verification): This process represents the steps taken when a user demands access to a service to determine whether the claimed identity matches the reference template. Firstly, a new biometric sample is acquired from the sensor, and then the features are extracted from the sample to generate the sample template, which is subsequently compared with the reference template (one-to-one for verification, one-to-N for identification). This comparison process generates a match score using a pattern classification method (e.g., a neural network). Finally, the match score value is compared

with a predefined threshold. If the match score value falls above the predefined threshold, system access will be permitted; otherwise, access is refused. Therefore, it is imperative to choose a discriminatory system threshold in order not to allow imposters to enter the system too easily, but that does not refuse legitimate users access to the system.

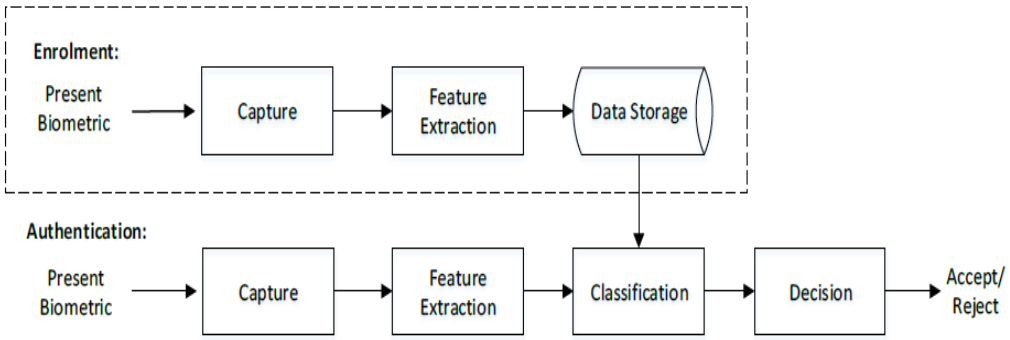


Figure 2-5: Generic biometric authentication system (Saevanee, 2014)

2.6.3 Biometric Performance Metrics

The performance of a typical biometric technique is measured by comparing a biometric sample from the current user with the existing reference template. These means of measurement are called the false acceptance rate (FAR), the false rejection rate (FRR) and the equal error rate (EER), as shown in Figure 2-6.

- The FAR refers to the percentage of access attempts by imposters that have been accepted by the system (i.e., incorrectly accepted). This is also called a type I error or false positive (sometimes referred to as the impostor pass rate). In this context, high FAR values are often seen as a significant problem because they represent an intrusion into a protected system.

- The FRR refers to the percentage of access attempts by legitimate users that have been rejected by the system (i.e., incorrectly rejected). This is also called a type II error or false negative (sometimes referred to as the *false alarm rate*).

- The true acceptance rate (TAR) is the rate at which the system correctly verifies the claimed individual.
- The true rejection rate (TRR) is the rate at which the system correctly rejects a false claim.

Generally, a low FAR indicates that the system is secure and a low FRR means the system is usable. The point at which the FAR and FRR are equal is called the EER, which means that a system is accurate. For a system to be considered accurate and to have performed well, it needs a low EER.

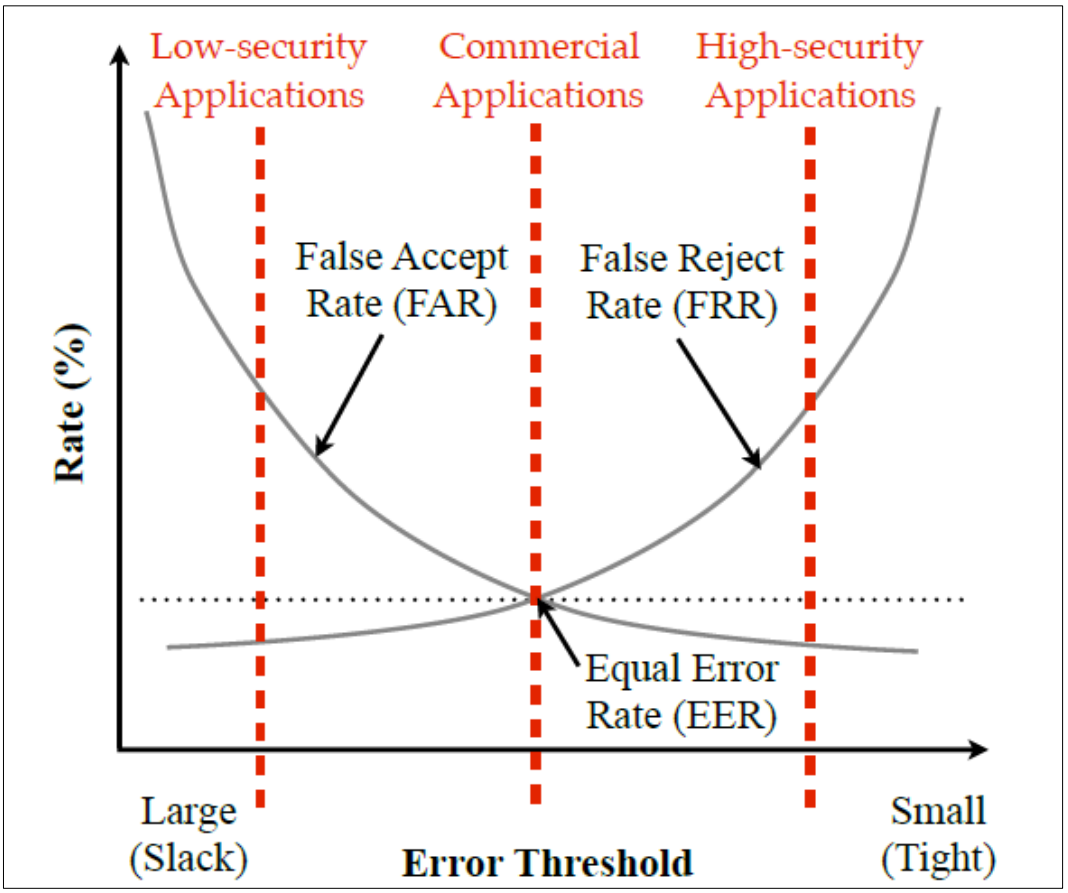


Figure 2-6: Biometric performance metrics factors (Crawford et al., 2013)

2.6.4 Biometric Techniques

Biometric authentication systems can be divided into two types: physiological or behavioural. Physiological biometric methods use a part of the human body to distinguish an individual based upon specific physical characteristics, such as the face, fingerprint, and iris. These physical features are more likely to remain constant over time and under different conditions. Furthermore, physiological biometrics naturally contain high levels of discriminative information and hence show a high degree of recognition performance. In comparison, behavioural biometrics refers to something the user does, such as typing, gait, application usage, voice, or signature (Woodward et al., 2003). Human behaviour is likely to change over time for several reasons, such as aging, fitness level, mood, and weather conditions; therefore, this might result in lower performance rates than physiological biometrics. However, this effect can be minimised if the template is regularly updated. To collect behavioural-based methods data, there is no need for special hardware and hence this may be cost effective. As a result, behavioural-based techniques are less unique but more flexible and convenient (Clarke, 2011). Furthermore, behavioural-based approaches perform better in the verification mode than they do in the identification mode.

2.6.4.1 Physiological Biometrics

A physiological biometric is one that is measured by gathering data from part of the user's body, such as by fingerprinting, iris and retina scans and facial recognition. Generally, these biometrics need a method for obtaining the data, such as the use of a scanner or camera.

- **Fingerprint recognition**: As a result of the uniqueness and permanency of human fingerprints, fingerprint recognition is one of the most accurate and commonly used biometric technologies (Jain et al., 2002; Woodward et al.,

2003). Furthermore, by 2015, fingerprint biometrics market revenue was expected to reach $3.28 billion (MarketsandMarkets, 2011). For instance, the Apple iPhone 5 added a Touch ID sensor to authenticate the user when trying to use the phone through the Home key. Unfortunately, fingerprints are sensitive to environmental conditions, such as age, dirt, and lost and therefore the performance of fingerprint recognition might be reduced (Jain et al., 2004). Furthermore, during the taking of user samples, there are a number of factors that might affect the surface of the fingertip, such as the positioning of the finger on the sensor and the amount of pressure exerted (Nanavati et al., 2002). The newer fingerprint readers are also boosted by a liveness sensor to decide whether the sample is taken from a living person or is fake (Clarke and Furnell, 2005).

- **Facial recognition:** Facial recognition is a method for identifying and verifying users by their face without any user interaction. This method is considered the second most popular after fingerprinting due to user adoption and the sale rate (Biometrics Institute 2013). The facial recognition approach is non-intrusive because user authentication could be performed without the user's knowledge by taking an image of the face from a distance. There are, however, some factors that might affect the system performance, such as the fact that the human face shape may change over time, lighting, and the possibility that a user may be too far away from the camera or his/her face obscured by glasses.

- **Iris recognition:** Iris recognition identifies a person using unique iris patterns by asking users to align their eyes with a camera, which may cause a certain level of inconvenience. However, an iris can be scanned through glasses and contact lenses (Woodward et al., 2003) and this procedure is 10 times more accurate

than fingerprint recognition (EPIC, 2005). Therefore, iris recognition is now considered the most secure and reliable biometric method (Jain et al., 2007).

- **Ear recognition**: Ear recognition is used to identify a user by the shape of the outer human ear while the user is making a telephone call, which is considered to be user-convenient because the ear image can be taken from a distance. Unfortunately, there are factors, such as when an ear is covered by an object (e.g., earrings), inconsistent lighting, accessories, and pose, that could affect the performance of the system. There is presently no commercial ear biometry product (Ross, 2011).

2.6.4.2 Behavioural Biometrics

Behavioural biometrics rely on a user's distinctive behaviours, such as typing, gait, touch screen interaction patterns, device use patterns and voice (Gupta et al., 2018). In this context, there is no need to use a device to collect the user data.

- **Keystroke analysis** (typing)**:** Keystroke dynamics is a behavioural biometric that is based on each person's individual typing style on a keyboard. It is taken by the measurement of such factors as the speed, frequency of characters, and the pressure with which keys are pressed (Karnan et al., 2011). When extracting keystroke activities, there are two main features that provide the most discriminative information (Clarke and Furnell, 2007): inter-keystroke latency (the time that elapses between releasing the first key and pressing the second) and hold time (the time interval between pressing and releasing a key), as shown in Figure 2-7.

Figure 2-7: Example of keystroke analysis

The keystroke approach can be performed in two modes:

- **Static** (text-dependent): A user's typing pattern is examined when certain keys are pressed, such as when entering a password.

- **Dynamic** (text-independent): There is no predetermined text (i.e., free text). Users are verified based upon their overall typing pattern, for instance, the typing rhythm speed. In this context, the resulting keystroke dynamic is likely to be more variable than a static keystroke.

- **Gait authentication:** Gait-based biometric authentication methods validate the user of a phone while walking, based on the person's gait, in a transparent and continuous manner, as shown in Figure 2-8. In this context, three types of gait recognition systems have been identified: machine vision-based, floor sensor-based, and wearable sensor-based techniques (Muaaz and Mayrhofer, 2013). The machine vision-based technique uses cameras from various distances to gather the user's gait data, whereas the floor sensor-based technique collects gait data from several sensors placed on floor mats, measuring aspects such

as pressure and force. Today, wearable sensor-based techniques are also identified as a new method for obtaining a user's gait data taking advantage of sensors built into mobile phones, such as accelerometers, gyroscopes, and force sensors.

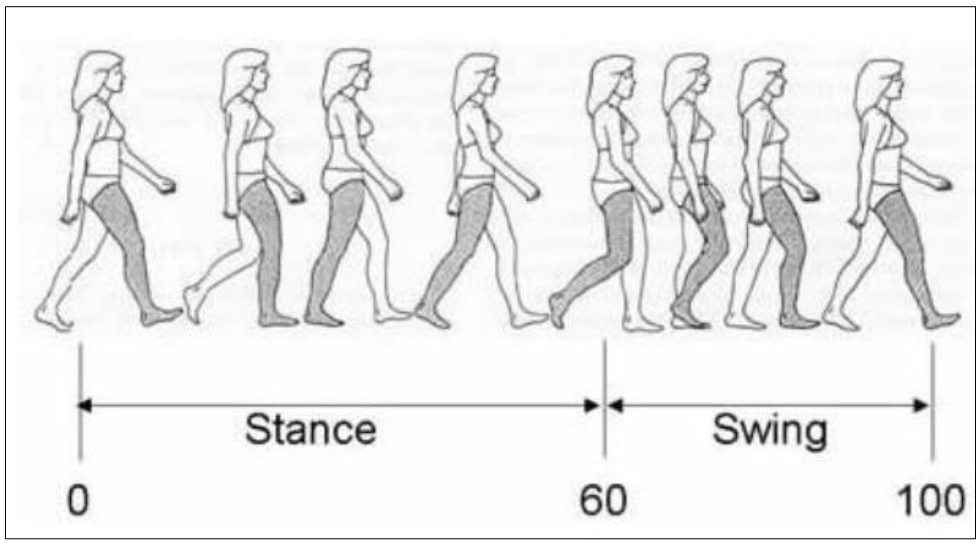


Figure 2-8: Gait cycle (Queen's University, 2011)

- **Voice verification** (speaker recognition): The way users speak can be used to verify their identity. Voice verification can, similar to keystroke dynamics, also operate in two modes: static (word-dependent, which requires a user to speak a predefined phrase) and dynamic (word-independent, which does not require any predefined phrases). There are some issues related to using a voice biometric to verify a user's identity, such as any changes in the human voice, surrounding temperature, mood, medication, and physical changes in the vocal tract. Therefore, voice biometrics are not suitable for large-scale deployment due to issues with contamination from other noise during recording.

- **Behavioural profiling** (service utilisation) attempts to identify and discriminate users based upon the way each user interacts with applications and/or services (Furnell et al., 2001); specifically, which applications they access, at what time of the day, and for how long. However, this technique is not expected to be unique and distinct enough to use as an identification system. Furthermore, it suffers from privacy issues during the behaviour monitoring, thereby affecting the level of user acceptance.

2.6.5 Multi-modal Biometrics

Uni-modal biometrics suffer from certain issues, such as noisy data, non-universality, spoof attacks, and unacceptable error rates (Ross and Jain, 2004). These weaknesses might be mitigated by multiple biometrics sources (Jain et al., 2005). Furthermore, if a user is not able to provide all the biometric samples required, multi-modal biometrics offer an opportunity to increase population coverage and, therefore, enhance overall system performance, reliability, and robustness (Jain et al., 2004). Typically, multibiometric systems can be classified into one of the following categories, as illustrated in Figure 2-9:

- **Multi-modal biometrics:** The multi-modal biometrics approach requires a combination of two or more biometric techniques, such as fingerprint and face recognition, or keystroke dynamics and behavioural profiling.

- **Multi-sample**: The multi-sample biometrics approach captures more than one sample of the same biometric trait, such as the frontal and side image of an individual face.

- **Multi-sensor:** The multi-sensor biometrics approach utilises more than one sensor to capture a single biometric modality of the user.

- **Multi-instance:** The multi-instance biometrics approach uses more than one subtype of the same biometric, such as the left index finger and the right index finger.

- **Multi-algorithm:** The multi-algorithm biometrics approach utilises more than one matcher algorithm in the classification process on a single biometric modality.

- **Hybrid:** In this approach, a subset of the above-mentioned categories is applied in order to optimise accuracy. For example, this could involve combining multi-modal and multi-algorithm systems (e.g., two voice recognition algorithms integrated with three face recognition algorithms).

Generally, there are some aspects to be considered when applying a multi-modal biometrics system, such as the number of traits, fusion level, the method of integration, and the data capture mode (Ross and Jain, 2004).

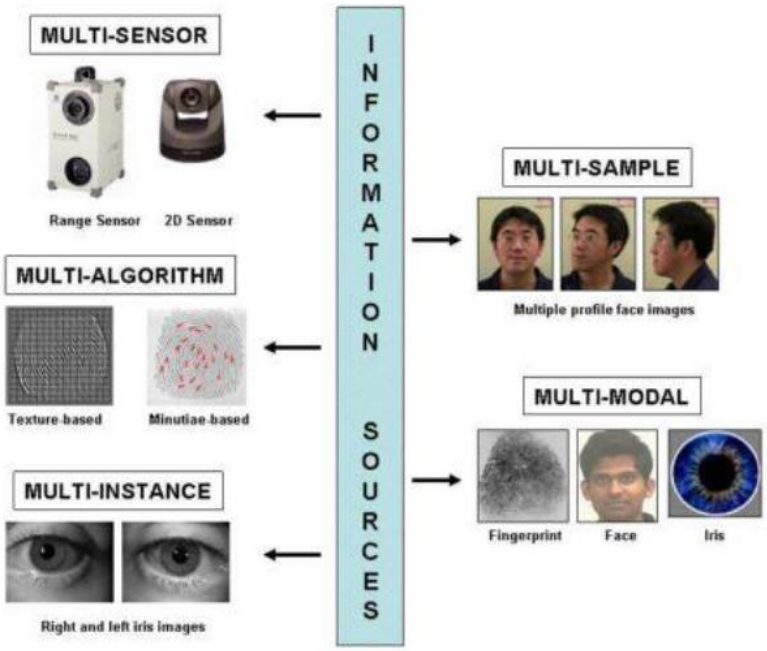


Figure 2-9: Sources of information for multibiometric systems (Ross 2006)

2.6.6 Fusion Biometrics

Biometric fusion refers to the combination of information from different sources, such as multi-modal, multi-instance, multi-sample, multi-sensor, multi-algorithmic, and hybrid approaches, in order to enhance the authentication decision and improve performance in a biometric system. As biometric systems are created from four main elements, namely, capturing the sample, feature extraction, template matching, and decision, biometric fusion could be implemented at the previous levels of the biometric process, including the feature level, matching level, or decision level (Ross and Govindarajan, 2005), as follows:

- **Sensor-level fusion**: Raw biometrics data are captured by multiple sensors and fused before being passed to the feature extraction phase. For example, fusing different face images from one or different cameras.
- **Feature-level fusion**: After capturing samples from one or more biometrics modalities, the feature vector is extracted from each sample and then these vectors are fused together. For example, fusing the feature vectors of the face and iris.
- **Matching score-level fusion**: The outputs of multiple biometrics classifiers are linked at this level to provide a new match score.
- **Decision fusion**: This level of fusion occurs when each biometric system has produced its own decision in order to enable the final decision.

2.7 Current Mobile Authentication Mechanisms

The most common form of mobile device security is based upon secret knowledge approaches, such as the use of passwords or PINs, although these are considered

inconvenient (Rodwell et al., 2007). This method is a point-of-entry technique, which means that the user has only to be verified at the beginning of a session. An imposter is then able to access all services, applications, and information without authentication. Furthermore, McAfee (2013) shows that the vast majority of respondents to their survey did not change the default password after purchasing a mobile device, the same passwords had been shared by one half of the users with others, and 15% saved their password on the mobile device itself. As a result, this technique is considered insufficient for safeguarding mobile devices (Kurkovsky and Syta, 2010). Similarly, with the Android password pattern, as demonstrated in Figure 2-10, the user is required to drag his/her finger across a touch screen on the three-by-three adjacent contact dots (i.e., make a connecting pattern rather than remembering a sequence of characters) to access the mobile device. The points can never be used as a combination again, thus producing fewer password combinations than the traditional PIN-based password technique. As a result, this method is vulnerable to a brute force attack (Aviv et al., 2010).

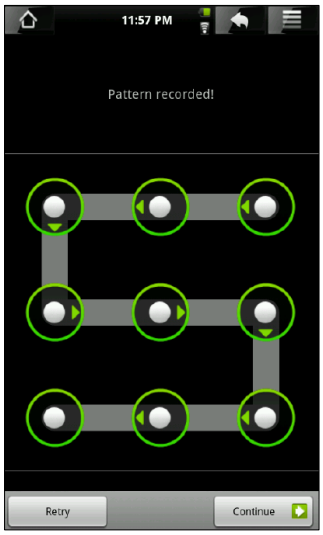


Figure 2-10: Android pattern lock (Meitiv, 2010)

With the evolution of mobile devices has come the introduction of a number of built-in features capable of sensing a variety of user biometric traits. These include features such as fingerprint readers or face recognition technology and are intended to provide a more secure authentication mechanism. Apple has presented a type of fingerprint technology to permit users to employ a fingerprint scan as a secure method of protecting their mobile device (Apple, 2014). In Touch ID, the user places the fingerprints (enrolling one or more fingers) onto the Home key and the system scans them in order to build a template, as demonstrated in Figure 2-11; later, in the authentication process, the user swipes his/her finger across the scanner to capture the fingerprint and authenticate it (Drummond, 2014). This approach is quick (it takes 30 seconds to enrol five fingers) and fairly reliable (Furnell and Clarke, 2014). Therefore, this approach has served to make the presence of Touch ID transparent and non-intrusive as a physiological technique (Juniper, 2018).

Figure 2-11. Fingerprint enrolment for iOS 7

Another example, as highlighted in Figure 2-12, is that Google presents face recognition technology (O'Boyle, 2014) by requiring the user to raise the phone and align his/her face to the camera until a match is made, which is considered an intrusive method compared with Touch ID.

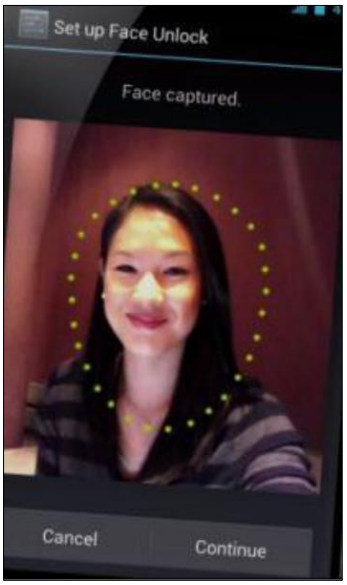


Figure 2-12: Android's face unlock feature (Wollaston, 2013)

Apple (2017) recently introduced a new technology to protect user information and securely and instantly unlock an iPhone X, called Face ID as shown in Figure 2-13, which has revolutionised authentication using facial recognition. This technology applies a TrueDepth Camera system to capture accurate face data and map the geometry of the user's face. Interestingly, this also enables payment approaches with Apple Pay. This technology also gives developers the opportunity to sign into their apps by utilising Face ID.

Figure 2-13: Face ID on iPhone X

Furthermore, Samsung has produced a new feature that the company calls Intelligent Scan, which can operate even in low light (Figure 2-14). This technology allows users to access their phone easily using convenient technology and makes unlocking simple by combining face recognition and iris scans (Samsung, 2017; CNET, 2018).

Figure 2-14: Iris scan on the Galaxy S9

Apple (2018) introduce an innovative dual-camera system (Dual 12MP rear cameras, 7MP TrueDepth front camera). The innovative technologies in the TrueDepth camera system work together in real time to recognise you in an instant. For instance, the Neural Engine uses machine learning to analyse data from the camera sensor, quickly distinguishing faces in the frame to detect the user face. The TrueDepth camera captures accurate face data by projecting and analysing over 30,000 invisible dots to create a depth map of your face and also captures an infrared image of your face. Once a face is detected, facial land marking allows iPhone to apply creative Portrait Lighting effects to your subject. Then, the ISP's advanced depth engine, combined with segmentation data from the Neural Engine, accurately separates your subject from the background.

On the other hand, Samsung (2018) produce a rear camera (12-MP Super Speed Dual Pixel) and front camera (8-MP). It's able to automatically switch between various lighting conditions with ease, making your photos look great whether it's bright or dark, day or night. For instance, On Galaxy S9 and Galaxy Note8, the available biometric authentication features are fingerprint scanning, face recognition, and iris scanning (Samsung 2018). In this approach, fingerprint scanning and face recognition are two quick and convenient unlock methods for your phone. In addition, there is also the option of a new fusion biometric authentication method called Intelligent Scan. By combining face recognition and iris scanning, it utilizes each to bolster the other depending on the environment—so in low light or broad daylight, you can unlock easily and securely. Intelligent Scan keeps your phone from prying eyes, while making it convenient for you to access it when you want.

Generally, in order for an authentication method to be considered an ideal alternative, it is important that it meets the following essential criteria (Elftmann, 2006): the

elimination of the need for additional hardware, a higher level of security, better memorability, simplicity and ease of use, and compatibility/applicability in various areas.

Chapter Three

Transparent Authentication Systems for Mobile Devices

3 Transparent Authentication Systems for Mobile Devices

3.1 Introduction

There is a high risk that, when a device is left on after the point-of-entry authentication stage (at login), requiring, for example, a PIN and password, an imposter can use the device to perform almost all tasks once successfully authenticated at the beginning of a session, without having to re-authenticate to validate the user's identity again periodically (Crawford et al., 2013). Furthermore, the current point-of-entry authentication mechanisms consider all activities on a mobile device to have the same level of importance and so maintain a single level of security for those activities, as illustrated in Figure 3-1, and do not apply any further access control rules (Clarke et al., 2009). Therefore, there is an urgent need to increase the level of authentication beyond the point-of-entry stage to verify the identity of the current mobile user in order to authenticate legitimate users in a continuous and transparent manner without the explicit involvement of the user or compromising convenience.

For the above reason, biometrics are considered a more usable approach that allows samples to be collected in the background without requiring deliberate actions from the user, in order to fulfil the need for an continuous authentication system. Accordingly, the use of biometrics to authenticate users transparently would improve the level of security and enhance usability (Clarke and Furnell, 2005). Therefore, Clarke and Furnell (2007) introduced a transparent and continuous authentication mechanism by gathering information from the owner of a device in an implicit manner to authenticate the user, as illustrated in Figure 3-2. In this approach, with each user contact with the mobile device, the system is able to collect user samples to gain a realistic measure of confidence regarding the identity of the user. Thus, this

transparent authentication method might be considered a remarkable solution to validating user identity with a higher level of security. However, although transparent authentication has a significant role to play in solving the flaw in verifying, there are a number of new problems, such as the cost and complexity of the system (Clarke, 2011), which need to be considered.

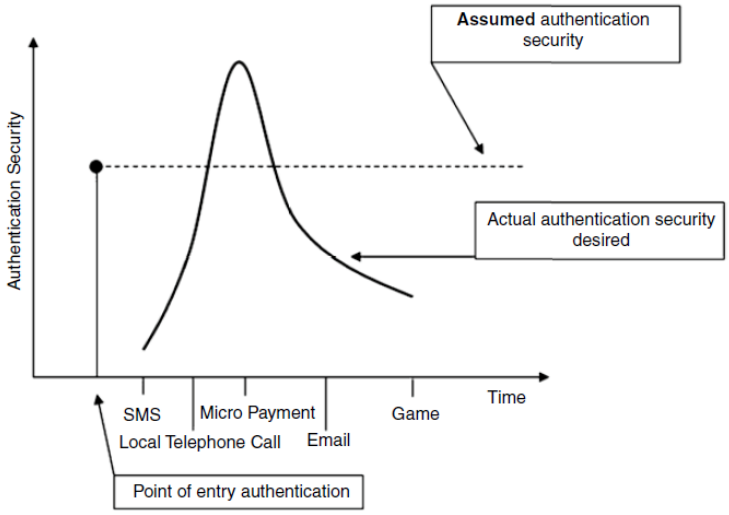


Figure 3-1: Traditional authentication security (Clarke, 2011)

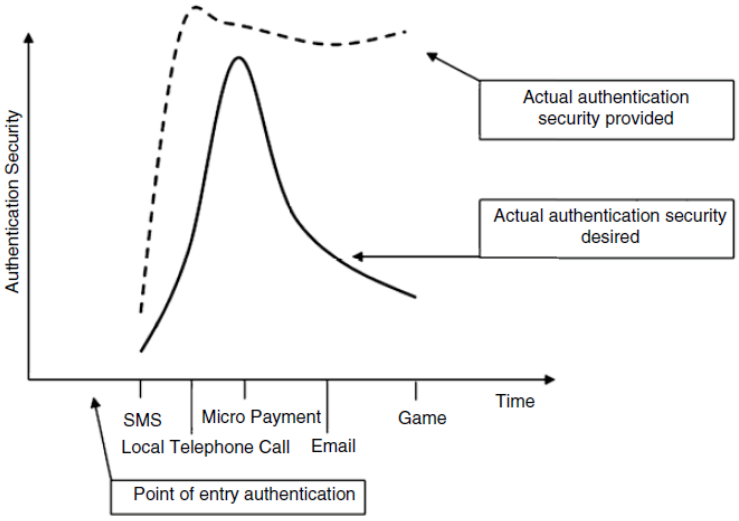


Figure 3-2: Model of continuous authentication confidence (Clarke, 2011)

Furthermore, 90% of the participants of one survey would have considered using transparent authentication on their mobile device if it were available to them, and 73%

considered transparent authentication a more secure approach than other traditional authentication methods (Crawford and Renaud, 2014). In this context, transparent authentication systems (TAS) have been described in various ways, such as implicit, passive, non-intrusive, unobtrusive, unobservable, active, and silent.

3.2 Uni-modal Transparent Authentication Systems for Mobile Devices

Transparent authentication systems for mobile devices can be classified by their use of physiological biometrics, such as fingerprint scanning or face recognition, or of behavioural biometrics, such as keystrokes or touch (Clarke et al., 2009; Chuang et al., 2018). Physiological biometrics are commonly considered useful for one-off authentication (Crawford and Renaud, 2014) because they require considerable computing power and high-quality images, which are not easy to obtain. Many efforts have been conducted in the literature to investigate the feasibility of using physiological biometrics to secure a mobile device without taking TAS into account (Tanviruzzaman and Ahamed, 2014). For instance, iris recognition needs the user to face the camera, takes more time for authentication and requires high-cost additional hardware (De Marsico et al., 2015). Moreover, there are still challenges for iris recognition, such as detection, segmentation, coding and matching and, therefore, iris scanning is considered an intrusive approach (De Marsico et al., 2014). Although fingerprint recognition suffers in the presence of poor conditions, such as cuts and dirt (Tang et al., 2010), modern mobile phones have embedded a fingerprint sensor to capture user samples transparently. Apple also introduced a new patent, called “Fingerprint Sensor in an Electronic Device”, in order to move the sensor from the Home key to a new location below the touch screen (Yousefpor et al., 2014). This will allow the reading of fingerprints from any point on the touch screen’s surface (Jakobsson et al., 2009). However, although face recognition suffers from some problems, such as being hard

to authenticate in the dark and changes over time (Tresadern et al., 2013), it is valid to apply it in a transparent authentication system because it could collect a sample without any effort from the user.

In contrast, behavioural biometrics refers to something you do, such as typing, gait, application usage, voice and signature, which is considered to be less sensitive to, for example, darkness or noise (Tanviruzzaman and Ahamed, 2014). In addition, user behaviour is gathered in the background without requiring dedicated activity from the user and by regularly and periodically checking user behaviour in order to monitor the protection of mobile devices continuously (Traoré and Ahmed, 2012). As a result, behavioural biometrics is presented as a suitable method, is more commonly used for transparent and continuous authentication, and provides usability (De Luca et al., 2012).

A mobile phone is able to provide the user's behavioural data, such as location, typing patterns, voice data and browsing patterns, without requiring deliberate actions from the user and without additional hardware. During the literature review, various behaviour-based authentications were presented as being able to verify the rightful owner of a device, such as touch screen input behaviour and keystroke, physical location, application usage, call and text, voice patterns, as well as micro-movement patterns due to the user's actions and gait patterns (Khan and Hengartner, 2014).

As highlighted in Table 3-1, it is clear that behavioural biometrics seems to be more transparent, with a lower authentication performance when compared with other, intrusive biometric approaches, such as iris and retina recognition, providing very high levels of performance.

Type	Technique	Transparent	Performance
Physiological	Ear geometry	* Yes	High
	Facial recognition	Yes	High
	Fingerprint recognition	Yes	Very High
	Iris recognition	No	Very High
	Retina recognition	No	Very High
Behavioural	Behavioural profiling	Yes	Low
	Speaker recognition	Yes	High
	Keystroke analysis	Yes	Low
	Gait recognition	Yes	Low
	Handwriting recognition	Yes	Medium

* Modified by the author : it means ear geometry has been considered transparent authentication recently

Table 3-1: Transparency of authentication approaches (Clarke, 2011)

A number of studies have been reported in the literature that investigate the feasibility of using behavioural biometrics to secure a mobile device. In this review, TAS for mobile devices have been summarised and classified into the following (Clarke et al., 2009; Chuang et al., 2018):

- Keystroke-based authentication
- Gait-based authentication
- Touch-based authentication
- Device sensor-based authentication
- Behavioural profiling-based authentication

3.2.1 Keystroke-based Authentication

Keystroke dynamics or typing rhythm has been used in the transparent authentication of the original user when typing characters on a keyboard, by utilising features such as key-hold time, latency, horizontal digraph, or vertical digraph. Considerable research has been undertaken of this approach. For example, Clarke et al. (2003) used a neural network classifier to study the feasibility of using keystroke dynamics to verify users' identity on mobile phones. The results of this work show that an FRR of 9.8% and a FAR of 11% can be achieved. As a follow-up study, Clarke and Furnell (2007) asked 30 participants to type telephone numbers and text messages to validate themselves as the mobile user, focusing on their typing characteristics – in particular, key-hold time and the number of times the backspace key was pressed. The authors reported that the average EER was 12.8%. In addition, Karatzouni and Clarke (2007) suggested applying a thumb-based keyboard approach on a mobile phone to authenticate 50 participants. Their findings demonstrated an average EER of 12.2% based on inter-keystroke latency, which is the interval between two successive keystrokes, using a feed forward multilayer perceptron neural network (FF-MLP).

Later, Zahid et al. (2009) selected six characteristic keystroke features: key-hold time, error rate, horizontal digraph, vertical digraph, non-adjacent horizontal digraph and non-adjacent vertical digraph. The results showed a best FAR of 2.07% and an FRR of 1.73%. However, the consequent degradation of response time in a mobile phone might negatively affect user acceptance. More recently, Burgbacher and Hinrichs (2014) suggested a classification framework for mobile phones via finger movement behaviour and typing on gesture keyboards, in order to decide whether a text message was written by the original user. Meanwhile, Draffin et al. (2014) focused on the specific location touched on each key, the drift from finger down to finger up, the force of touch,

and the area of press (i.e., based on how the user types). Using keystroke dynamics is a transparent approach for authenticating a mobile user, and there is no need to use specific hardware to capture the data. However, it is difficult for a keystroke dynamics system to achieve authentication in a consistent way if the user types unusually and this could be replaced by touch screen mobile phones (De Marsico et al., 2015).

Recently, Xiaofeng et al. (2019) employs a model of a Convolutional Neural Network (CNN) and a Recurrent Neural Network (RNN) to learn the keystroke data of free texts to carry on continuous authentication. In this study, the authors divide the user keystroke data into a fixed-length keystroke sequence, and convert the keystroke sequence into a keystroke vector sequence according to the time feature of the keystroke (Xiaofeng et al, 2019). The Buffalo dataset (sun et al, 2016) is used in this research study. This dataset contains 157 participants' long fixed text and free text keystroke data. According to (Xiaofeng et al. 2019), the participants completed inputting through 3 sessions, and each participant has an average of 5,700 keystrokes in each session. The average of total 3 sessions have exceeded 17,000 keystrokes. A model of a recursive neural network plus a convolutional neural network is used to learn a sequence of individual keystroke vectors to obtain individual keystroke features for identity authentication. The findings of this study were Equal Error Rate (EER) was 3.04%, False Acceptance Rate (FAR) was 4.12%, and False Rejection Rate (FRR) was 1.95%.

3.2.2 Gait-based Authentication

Gait-based biometric authentication methods validate, in a transparent and continuous manner, the user of a phone while walking based on his/her gait. In this context, three types of gait recognition systems have been identified: machine vision-based, floor sensor-based, and wearable sensor-based techniques (Muaaz and Mayrhofer, 2013).

The machine vision-based technique uses cameras from various distances to gather the user's gait data, whereas the floor sensor-based technique collects gait data from several sensors placed on floor mats, measuring aspects such as pressure and force. Today, wearable sensor-based techniques are also identified as a new method to obtain a user's gait data, taking advantage of sensors built into mobile phones such as accelerometers, gyroscopes, and force sensors.

Some investigation efforts have been made in the literature to introduce gait recognition as a behavioural biometrics authentication approach. For example, Derawi et al. (2010) conducted two short sessions to authenticate a mobile user by asking 51 users to walk up and down with a mobile device placed at the hip, in order to gather user data. This achieved an EER of 20%. In addition, Gafurov (2004) pointed out some issues facing gait authentication as a robust modality, such as clothing, shoes, sensor sampling rate, phone placement and orientation. To solve orientation error, which is caused by the mobile phone vibrating inside the pocket, and the noise cancellation issue, Muaaz and Mayrhofer (2014) asked 35 participants to place their mobile phone inside their right front trouser pocket in a realistic scenario and walk 68 meters along a straight corridor with no stairs. In previous studies, acceleration data were collected in the same location (i.e., in a pocket in a fixed manner, or on the hip, ankle, or arm). In practice, a mobile phone may be held in a variety of ways; for example, a user may be calling or touching the screen while walking. Therefore, the direction of the mobile phone should be taken into account in these situations (Muaaz and Mayrhofer, 2014). Unlike previous work, Hoang and Choi (2014) asked a total of 34 volunteers to complete around 18 laps, change their footwear and clothes, and wear trousers with narrow pockets in order to prevent the mobile phone changing position and orientation, which is not practical. The FAR was 35%, which is considered a drawback of this work.

Using gait authentication to identify the user in a usable way by means of an accelerometer sensor, which can deliver data along three axes (x, y, z), may have some advantages. However, it is still under development, needs more investigation and must address some of the challenges which may affect performance, such as when the user is not walking, terrain, injury, footwear, fatigue, and personal idiosyncrasies (De Marsico et al., 2015). It is reasonable, therefore, to combine this approach with another modality to increase accuracy and performance.

Al-Obaidi et al. (2018) investigate the performance of gait recognition across a wider range of activities and upon 60 participants across a multi-day. In this study, each participant was asked to walk normally, fast with a bag on flat ground for three minutes for each activity, and then to walk down stairs for three levels and upstairs for three levels on a predefined route and stop for 15 to 20 seconds between activities. According to Al-Obaidi et al. (2018), 10 sessions of user's activities were collected per user: 5 sessions were from one day and the other 5 sessions were collected a week later. Finally, five datasets collected to each activity (normal walk, fast walk, and walk with a bag, downstairs walking, and upstairs walking). Totally, 68 samples were collected for each user per day; and in total 8,160 samples were collected for the entire dataset Al-Obaidi et al. (2018). Two experiments were be done by the authors. Firstly, the first experiment explores the classification performance of individual activities in order to understand whether a single classifier or multi-algorithmic approach would provide a better level of performance. The results from the experimentation was shown an EER of 12.2 % for a single classifier. On the other hand, the second experiment was a multi-algorithmic approach where different classifiers are used based upon the nature of the activity (Al-Obaidi et al, 2018). In this context, the multi-algorithmic

approach achieved EERs of 6.3% (normal), 12.68% (fast) and 6.46% (a bag walk) using both accelerometer and gyroscope-based features.

3.2.3 Touch-based Authentication

A variety of studies have been proposed in this domain. For example, Zheng et al. (2014) used a combination of acceleration, pressure, size and time, which could be collected from sensors in touch screen mobile phones. They claim this approach is a non-intrusive authentication method, in contrast with asking the user to insert a 4-digit or 8-digit PIN. This does not provide a complete transparent authentication system. Two similar research projects, Frank et al. (2013) and Li et al. (2013), also examined user authentication on a mobile phone by continuously observing finger movements on a touch screen. The latter work focused on sliding behaviour in gestures (left, right, up, and down) without requiring any deliberate action from the user. However, this employs a two-class classifier, which is considered an unrealistic method, since it requires input data from non-owner users at the training phase. In comparison, the classification framework used by Frank et al. (2013) (called Touchalytics) had EERs between 0 and 4% from 41 participants.

In a comparable setting, the FAST (Finger gestures Authentication System using Touchscreen) system gathers information about multi-touch user gestures (i.e., flick, pinch, spread, drag, rotate) using a sensor in a post-login setting (Frank et al., 2013). The authors selected a total of 53 features for each touch gesture, and FAST accomplished an FAR of 4.66% and an FRR of 0.13%, although utilising the associated digital glove might be impractical. Unlike the previous work, Feng et al. (2014) studied touch screen gestures in the context of running an application in a transparent fashion and presented a novel Touch-Based Identity Protection Service (called TIPS). TIPS achieved up to 90% accuracy and battery usage of 6% in

authenticating a user, without employing motion sensor data, in order to reduce power consumption. In this context, some prior researchers, such as Frank et al. (2013), required users to accomplish predefined touch gestures, or collected data in controlled environments which do not represent natural user interactions. However, the TIPS framework carries out implicit real-time user identification (Feng et al., 2014).

Similarly, in line with providing touch-based behavioural authentication, Shahzad et al. (2013) presented a gesture-based authentication scheme called GEAT, based on how multi-touch gestures are input, for a secure unlocking mechanism on the login screen, which is unsuitable for a transparent authentication system. Later, Draffin et al. (2014) focused on the specific location touched on each key, the drift from finger down to finger up, the force of touch, and the area of press (i.e., the way the user types). To evaluate this, they envisioned an application called KeySens, which develops a model of a user's micro-behaviour and can detect when the phone is in a different person's hands. However, they performed this experiment for three weeks without declaring the performance.

Concurrent work conducted by Xu et al. (2014) showed that the slide gesture was considered the best technique, achieving an EER of less than 1% compared with other touch operations, such as pinch, handwriting and keystroke. Cheng et al. (2013) claimed that touch-based biometrics are ineffective due to the micro-movement of mobile devices caused by touch when the user is mobile.

Filippov et al. (2018) suggest a Continuous user authentication based on the features of their interaction with the device's touch screen. The research study was collected the data from twenty-one users upon the features of interaction with a touch screen. After the feature extraction and the Isolation Forest method training the values of FAR and FRR equal to 7.5% and 6.4%, respectively, were obtained. Similarly, Alghamdi

and Elrefaei (2018) proposes a dynamic authentication of mobile phone users based on their gestures on touchscreen for of twenty participants. In this study, tapping, scrolling, dragging and zooming gestures' data were acquired using a developed android application. Each participant is required to be familiar with a mobile that is equipped with a touchscreen. Five sessions were recorded for every participant. For each user, forty-two features, eleven features from tap gesture, sixteen features from both scroll and drag gestures, and fifteen features from zoom gesture were extracted from the collected touch gestures. Three different Classifiers namely medians vector proximity (MVP), k-nearest neighbour (k-NN) and random forest (RF), were applied to the extracted features. The experimental results demonstrate that MVP classifier achieves the best results when using single gestures and achieve EER 5.25%. The k-NN gives the best results when two gestures are combined together, finally the k-NN classifier using only three gestures.

Modality	No	Reference (Year)	Performance (%)			# User	Time
			EER	FAR	FRR		
Keystroke	1	Clarke and Furnell (2007)	5	n/a [i]		32	3 sessions
	2	Karatzouni and Clarke (2007)	12.2	n/a		50	n/a
	3	Zahid et al. (2009)	2	2.07	1.73	25	n/a
	4	Maiorana et al. (2011)	4.4	n/a		40	n/a
	5	Trojahn and Ortmeier (2013)	2	11	16	18	n/a
	6	Burgbacher and Hinrichs (2014)	0	n/a		16	4 weeks
	7	Draffin et al. (2014)	n/a	14	2.2	13	3 weeks
	8	Xiaofeng et al. (2019)	3.04	4.12	1.95	157	28 days
Gait	9	Derawi et al. (2010)	20	n/a		51	2 sessions
	10	Nickel et al. (2012)	8.24	n/a		36	n/a
	11	Muaaz and Mayrhofer (2014)	7.051	n/a		35	n/a
	12	Hoang and Choi (2014)	3.5	16.2	3.5	34	n/a
	13	Al-Obaidi et al, (2018)	0.7	n/a		60	2 days(10session)
Touch	14	Feng et al. (2012)	n/a	4.66	n/a	40	n/a
	15	Frank et al. (2013)	< 4	n/a		41	1 week
	16	Shahzad et al. (2013)	0.5	n/a		50	n/a
	17	Li et al. (2013)	3	3	3	75	n/a
	18	Cai et al. (2013)	4	4.05	3.27	20	n/a
	19	Xu et al. (2014)	< 10	n/a		31	1 month
	20	Zheng et al. (2014)	3.65	n/a		80	n/a
	21	Feng et al. (2014)	10	n/a		23	n/a
	22	Shen et al. (2014)	< 8	4.68	1.17	51	n/a
	23	Filippov et al, 2018	n/a	7.5	6.4	21	1 month
	24	Alghamdi and Elrefaei (2018)	5.2	n/a		20	n/a
	25	Yang et al, (2019)	4.15	n/a		45	2 weeks
Device sensors	26	Conti et al. (2011)	n/a	4.44	9.33	10	n/a
	27	Lin et al. (2012)	6.85	n/a		20	n/a
	28	Zhu et al. (2013)	25	n/a		20	n/a
	29	Lee and Lee (2015)	10	n/a		4	3 weeks
	30	Hong et al. (2015)	n/a	7.17	3.67	8	8 weeks
	31	Wang et al. (2015)	n/a	< 2.5	< 2.5	50	30 mins / user
	32	Sitova et al. (2015)	6.92	n/a		100	n/a
	33	Yang et al. (2015)	n/a	15	10	200	10 sec * 3 times
	34	Neverova et al. (2016)	20	n/a		n/a	
	35	Zhu et al. (2017)	1.2	n/a		20	months
	36	Buriro et al. (2017)	4	n/a		53	n/a
	37	Ehatisham et al. (2018)	2.05	n/a		4	n/a
	38	Shen et al. (2019)	n/a	5.03	3.98	102	n/a
Behavioural profiling	39	Shi et al. (2011)	n/a			50	12 days
	40	Hayashi et al. (2012)	structured interviews			20	Each interview 90 minutes
	41	Khan and Hengartner (2014)	application-centric			30	4 different dataset
	42	Li et al. (2014)	n/a	4.17	11.45	76	n/a
	43	Kayacık et al (2014)	n/a				3 different dataset
	44	Ryu et al (2018)	2.41	n/a		22	42 days
	45	Zhao et al (2018)	15	n/a		130	n/a
	46	Alotaibi et al (2019)	26.9	n/a		76	1 month

Note: n/a = not applicable

Table 3-2: Uni-modal transparent authentication systems for mobile devices

3.2.4 Device Sensor-based Authentication

A number of studies have investigated the leveraging of multiple sensors on smartphones. For example, Conti et al. (2011) utilised the accelerometers and gyroscopes in a smartphone to verify the user while the user is making a phone call. From this perspective, it is inconvenient to authenticate users when they want to use their mobile phone and need to perform specific movements. Yang et al. (2015) focus on arm length and wrist size and propose a hand-waving biometric-based authentication method, developing a prototype called Open Sesame to utilise users' waving patterns for locking and unlocking using the accelerometer sensor. The findings demonstrate an average FAR of 15% and an FRR of less than 8%, which are considered higher than the results achieved by Conti et al. (2011). Later, combining touch, accelerometer, and gyroscope sensor data, Wang et al. (2015) suggested that sensor fingerprints could be a feasible solution for user verification and introduced two new unlocking gestures for sensor-based user authentication based on a sensor fingerprint. The authors show an FAR and FRR of less than 2.5%.

Further studies in a similar context, relying only on a multi-sensor approach, were separately introduced by Lin et al. (2012), Lee and Lee (2015), and Sitova et al. (2015). The first study argues that multiple sensor inputs could improve accuracy over that of a single sensor and present a non-intrusive authentication approach based on orientation sensor (i.e., gyroscope sensor) data taken from the pitch, roll, and heading, based on how users holds their phone. Zhu et al. (2013) propose SenSec, an implicit authentication framework that captures passive sensory data from a mobile device; namely, an accelerometer, orientation, compass, and gyroscope, which determine where the user is and what he/she is doing. The researchers asked users to perform specific tasks in a sequential order, which was considered impractical. SenSec is a

similar system to SenGuard (Shi et al., 2011), which is a non-intrusive authentication system based on four sensors: accelerometer, location, multi-touch screen, and voice. SenGuard obtained very good user authentication results with an average error rate of 3.6% (Shi et al., 2011). Nonetheless, the power consumption of the system may be one of the major issues for this work. In the same context, the Global Positioning System (GPS) could cause the quick draining of a battery but gait recognition has a reasonable cost, which means that not all sensors cause battery drainage, with an EER of 10% (Yousefpor et al., 2014).

Using deep neural networks, Neverova et al. (2016) proposed a scheme for learning human identity based on their motion patterns and achieved an EER of 20%. Zhu et al. (2017) introduce a novel user authentication scheme called ShakeIn. This approach is a handy user authentication scheme for secure unlocking of a smartphone by simply shaking the phone. The experiments were performed on 20 participants with 530,555 shaking samples in total collected over multiple months. The results show that ShakeIn achieves an EER of 1.2% on average. Similarly, Buriro et al. (2017) collects data from multiple 3-dimensional smartphone sensors in the background for a specific period of time and profiles a user based on the collected hand movement patterns for authentication purpose. The data were collected from multiple sensors, namely, accelerometer, gravity, gyroscope, magnetometer, and orientation of 53 participants. The Random Forest classifier was used for evaluating the results which was An EER of 4%.

In the same context, Ehatisham et al. (2018) propose a novel continuous authentication scheme to recognize smartphone users on the basis of their physical activity patterns using accelerometer, gyroscope, and magnetometer sensors of smartphone. In this study, identifies the users based on the way they perform certain

activities using mobile sensing. According to Ehatisham et al. (2018), six activities of daily life such as walking, running, sitting, standing, walking upstairs, and walking downstairs, are used to distinguish between different users based on sixteen different features extracted from the time domain. Five different positions are employed for keeping a smartphone on the user's body and the user recognition results are analysed for all these positions (Ehatisham et al. 2018). Three different classifiers namely Support Vector Machine (SVM), Decision Tree (DT), and K-Nearest Neighbours (K-NN), are performed for user recognition. SVM classifier achieved the best results for user recognition with an overall average accuracy of 97.95%. Likewise, Shen et al. (2019) develop a Markov-based classifier to model motion-sensor data sequences for active smartphone authentication. The findings show that the system achieve a false-rejection rate of 5.03% and a false-acceptance rate of 3.98%.

3.2.5 Behavioural Profiling-based Authentication

Studies have proposed application usage aimed at providing transparent authentication. For example, Hayashi et al. (2012) argue that device-centric continuous authentication cannot discriminate between data from different applications. More broadly, the authors argue that this method cannot make any assumptions in terms of the importance of the application currently being used. More specifically, the lack of a device-centric approach, and being unaware of the task that the user is performing within an application, can lead to not delivering authentication control at the task level (De Luca et al., 2014). This will lead to a higher authentication overhead. Hayashi et al. (2012) argue the inefficiency of the all-or-nothing access model and suggest that a mobile user should be authenticated only when a sensitive application is begun, since most applications do not require explicit authentication. In the context of a sensitive application concept, the authors created paper prototypes

(i.e., a theoretical method) of two alternative access mechanisms: group accounts and an activity lock. The group account would provide access to some of the functionality that is normally available only when the phone is unlocked and is thus for sharing non-sensitive information or applications; whereas an activity lock can be activated by the device owner before handing the device to another user to share specific screens in an application. Conversely, configuring a group account on a device enables a device's owner to share a specific set of applications with other users.

In the same context, the work of Riva et al. (2012) is based on when the user should authenticate (as opposed to how) and for which application. The authentication decision depends on the confidence and sensitivity levels relating to each application, which are stated by the user to protect sensitive applications from unauthorised use. The result of this prototype was a 42% reduction in requested explicit authentication, but was only conducted with nine users. A similar but more extensive study was conducted on positive habits (i.e., familiar events) and negative habits (i.e., unexpected changes of predictable places). Shi et al. (2011b) recorded a user's routine, such as location, phone calls, and application usage, in order to build a profile and assign a positive or negative score for each user's routine.

Among further studies in a similar context, Li et al. (2011) introduced a behaviour profiling approach to identify mobile device misuse by focusing on the mobile user's application usage; namely, general application use, voice calls, and text messaging. The total EER was 7.03%. Later, the authors (Li et al., 2014) presented a novel behaviour profiling framework able to collect user behaviour to evaluate the system security status of a device in a continuous manner before accessing sensitive services. They investigated the sensitivity of the application concept, which is mapped to high-risk levels, to render the framework more secure and transparent when the user

requires access to high-value applications. This in turn means that the system will reject user access after several attempts at using different applications, rather than a single attempted application use. The authors conclude that the system seems to be able to distinguish mobile users through their application usage; in particular, by focusing on the names of applications and the location of usage, which are considered valuable features. However, the MIT Reality dataset was created in 2004 with a small number of mobile applications, causing difficulty in discriminating between users. This is considered the main limitation of this dataset.

Zhao et al. (2018) propose an improved Bayesian network model and linear model to predict what application to use next time only consider time and latest used application on text to study the user behaviour. The evaluation results show that the accuracy of this model can be achieved 85%. Likewise, Alotaibi et al. (2019) presents a novel behavioural profiling approach to user identity verification as part of mobile application security. Using a machine learning classifier, the predictable model created is able to authenticate the mobile user based on his/her behaviour. Supervised learning methods were chosen in this experiment due to the labelled known data and known responses. Three classifiers were selected in this research study: a support vector machine (SVM), random forest (RF), and gradient boosting (GB), to identify the most efficient machine learning classifier based on the classifier output. The experimental results show that users could be distinguished via their behavioural profiling upon each action within the application, with an average equal error rate of 26.98% and the (GB) gradient boosting classifier results prove quite compelling.

3.3 Multi-modal Transparent Authentication Systems for Mobile Devices

Investigations have been conducted in the literature into the feasibility of combining biometric modalities to authenticate the mobile user, as shown in Table 3-3. Clarke

and Furnell (2007) offered a mobile-based system, the Intelligent Authentication Management System (IAMS), by means of grouping together a secret knowledge-based method and available biometrics modalities. As a follow-up study, Clarke et al. (2009) proposed a framework called Non-Intrusive Continuous Authentication (NICA) to provide secure, transparent and continuous authentication. NICA uses keystroke dynamics, facial recognition and voice patterns to inform an Alert Level while the user interacts with the mobile device. NICA is based on 'authentication confidence', which is mapped to each service in order to allow the user to access a service if confidence levels are higher than the alert level. To evaluate this framework, the authors conducted an experiment with a NICA prototype, in which 27 participants were asked to perform specific tasks for 45 minutes; the result was an EER under 0.01%. In this work, the authors considered the hypothesis that different services require different levels of security and protection by understanding the risks associated with specific user actions and services, such as transferring money from an online banking application.

Building upon the work by Clarke and Furnell (2007), Crawford et al. (2013) introduced a transparent authentication framework utilising a combination of behavioural biometrics: keystroke dynamics and voice recognition, based on device confidence level. In this research, each task on the device was assigned a particular device confidence level as the minimum threshold for access to the task, either explicitly by the owner or by default. As a result, private or sensitive information could be accessed only at the highest device confidence levels. This method is similar to online banking systems for which the user needs to perform a task that might have side effects; the bank system requires a further authentication step from the user before the user can be authorised (Crawford et al., 2013). The authors did not, however, show the total

EER performance for this multi-modal behavioural biometric. However, if the device confidence level is less than the required task confidence level, the user must try to raise the level of the device confidence in order to be authorised. Therefore, this step will lead the user to use a second authentication action in an explicit manner, such as a password or physiological biometric. The authors also assume there is one mobile device for each user, which might not be the case.

Similarly, Saevanee et al. (2012) examine a combination of three diverse biometric methods: keystroke dynamics, behavioural profiling and linguistic profiling. By using this multi-modality, they achieved a total EER of 3.3% from 30 virtual users (this dataset was not real and was gathered from different datasets). To continue their work, Saevanee et al. (2014) presented a text-based authentication framework utilising the modalities and introduced a security level by allowing the user to set security levels for access to different applications. The authors claim that this approach would reduce the number of intrusive authentication requests for high security applications by 91%. Likewise, Fridman et al. (2015) propose a parallel binary decision-level fusion architecture for active authentication. The fusion is used for classifiers based on four biometric modalities: text analysis, application usage patterns, web browsing behaviour, and the physical location of the device by computing GPS (outdoors) or Wi-Fi (indoors). To evaluate this framework, the authors collected a dataset from 200 users' Android mobile devices for 30 days, which is considered a large dataset in the transparent authentication literature. After 1 minute of the user using the device, the ERR was 5%, whereas after 30 minutes the EER was 1%. Despite the promising results in this work, battery consumption was a major issue.

From a different perspective, there are some frameworks that aim to facilitate users moving from one device to another without asking them to authenticate. In this context,

Hocking et al. (2011) introduced the Authentication Aura concept, which is based on the enabling of cooperative and distributive authentication between devices owned by a single user. The results suggest that this concept could reduce the number of intrusive authentication requests by up to 74%.

Building upon the concept of an Authentication Aura, Al Abdulwahid et al. (2013) suggest a conceptual authentication model hosted in the cloud, called Federated Authentication, which would act as a centralised Managed Authentication Service Provider (MASP). The main principle of this model is to take advantage of cloud computing features, such as scalability, universality and adaptability, as a means to reduce the need for logging onto and authenticating on each device in a transparent and continuous manner. However, certain aspects need to be considered, such as privacy, trust, and response time, in order to make this model more secure and practicable.

Recently, Lamiche et al (2018) propose a new multimodal authentication method able to strengthen the smartphone authentication system based on gait patterns and keystroke dynamics without user intervention through simultaneous walk and text input. In order to build a multimodal biometrics profile for the user, a feature level fusion method is applied. According to Lamiche et al (2018), the data was collected from 20 participants in a single session under a controlled environment and about 63,500 samples from the accelerometer sensor and 8600 keystrokes were collected from all 20participants. Using different machine learning classifiers namely, support vector machines (SVM), random forest (RF), random tree (RT), Naïve Bayes (NB) and multilayer perceptron (MLP), the proposed method is examined. The experimental results achieved a promising EER of 1% when using (MLP) multilayer perceptron classifier with the average false acceptance rate, and false rejection rate values of 1.7

%, 7%, respectively. Likewise, Acien et al (2019) propose MultiLock (Mobile Active Authentication based on Multiple Biometric and Behavioral Patterns) by considering seven different data channels and their combination. These modalities were Touch dynamics (touch gestures and keystroking), accelerometer, gyroscope, WiFi, GPS location and app usage were all collected during human-mobile interaction to authenticate the users. This study used UMDAA-02 database which Comprises 141.14 GB of smartphone sensor signals collected from 48 Maryland University students over a period of 2 months in unsupervised scenario. According to Acien et al (2019), the sensors captured are touchscreen, gyroscope, accelerometer, magnetometer, light sensor, GPS, and WiFi, among others. Information related to mobile user´s behavior like lock and unlock time events, start and end time stamps of calls and app usage are also stored. The result was achieved 3% of EER.

No	Reference (Year)	Multi-modality			Performance EER (%)	# Users	Time
1	Clarke et al. (2009)	Face	Voice	Keystroke	Total: 0.01	27	45 minutes
2	Shi et al. (2011)	Accelerometer		GPS location	Average: 3.6	50	2 weeks
		Touch screen		Microphone			
3	Ketabdar et al. (2011)	Movement		Audio	2.5	9	2 minutes / user
4	Crouse et al. (2013)	Face capture		Gyroscope	n/a*	24	n/a
		Accelerometer		Magnetometer			
5	Crawford et al. (2013)	Keystroke		Voice pattern	10	30	n/a
6	Bo et al. (2014)	Touch		Accelerometer	< 1	100	n/a
		Gyroscope					
7	Saevanee et al. (2012) Saevanee et al. (2014)	Behavioural profiling			9.2	30	n/a
		Linguistic profiling			12.8		
		Keystroke			20.8		
		Overall			3.3		
8	Tanviruzzaman and Ahamed (2014)	Gait		Location tracks	10	13	1 week for gait 2 weeks for location
9	Fridman et al. (2015)	Linguistic analysis		Behaviour profiling	1 after 30 minutes	200	30 days
10	Lamiche et al (2018)	Gait		Keystroke	(FAR =1.7 ,FRR= 7)	20	n/a
11	Acien et al (2019)	Touch	GPS	Keystroke	3	48	2 months
		App usage	Wi-Fi	Accelerometer			

Note: n/a = not applicable

Table 3-3: Multi-modal transparent authentication systems for mobile devices

3.4 Discussion

According to the above comprehensive analysis of a review of the literature on transparent authentication systems for mobile device security, some physiological biometrics suffer from issues such as poor image quality, usually requiring additional hardware, and consuming a great deal of power. However, studies have found that behavioural biometrics can operate transparent and continuous authentication by constructing a user behavioural profile while the user is using the device, without requiring deliberate actions from the legitimate user. In addition, the majority of recent research in this domain has focused on finding appropriate behaviour-based classifiers for a transparent authentication approach, such as the use of keystroke, gait, touch, and sensors. However, issues with these methods, such as energy consumption, mean that it is considered a great challenge to use multiple sensors to verify a user's identity. Choosing suitable sensors to collect behavioural data using this method would lessen further costs in terms of the device's central processing unit (CPU) and battery life. Moreover, when the user is mobile, the micro-movement of the mobile device could affect the performance of touch-based biometrics and cause a high error rate. As such, a touch approach might be vulnerable to shoulder-surfing attacks. As shown in Table 3-2, although many studies have investigated utilising touch and sensor approaches in order to authenticate whether a user is the owner of the smartphone, a number of further issues need to be considered. For instance, various studies had a small number of participants and no general security performance results were declared for some of the studies, which makes comparison difficult.

In addition, there is a lack of investigation and study of behavioural profiling and, in particular, application usage for transparent authentication systems on mobile devices,

as Table 3-2 illustrates. Furthermore, today, many applications have been produced whose properties could be beneficial, such as online social networks. A great deal of information could usefully be collected from user behaviour; specifically, by focusing on the sensitivity level of the application, understanding whether a certain application may require protection, and studying user behaviour and interaction with each application. On the other hand, this technique is not expected to be unique or distinct enough to fulfil the need for a continuous authentication system. It also suffers from privacy issues during behaviour monitoring, thereby affecting the level of user acceptance. Likewise, device-centric behavioural biometric authentication approaches apply a specific classifier without taking into account the nature of the applications currently being used to verify user identity. More specifically, gate authentication is not suitable for authenticating a mobile user when the text message application is being used, whereas keystroke is suitable for authentication. Even if a multi-classifier system were employed for collecting user behaviour data from different applications, this would lead to a higher authentication overhead.

As mentioned previously, the current point-of-entry authentication mechanisms consider all applications on a mobile device to have the same level of importance and maintain a single level of security for all applications, thereby not applying any further access control rules. Moreover, only a few studies have investigated when to authenticate a mobile user. For instance, it is unnecessary to authenticate a user when reading the news or checking the weather forecast through a browser application. However, those studies used an old dataset, which might not resemble the real use of such a system. Therefore, this approach could result in reducing unnecessary authentication overhead by focusing on the sensitivity of the process within the application. Consequently, a smarter biometric approach that is able to categorise data

from different applications and knows what interactions the user is performing within the application will reduce the authentication overhead.

Unlike previous works, this research argues that, on a single mobile application, different processes operate on the same data with a different social risk based on the user action. More specifically, the unauthorised disclosure or modification of mobile applications data has the potential to lead to a number of undesirable consequences for the user, which, in turn, means that the risk changes within the application. Thus, there is no single risk to using a single application. This work also suggests there is a need to move an access control system from a position on the application to within the application based on the risk for each user action. Therefore, there is a need to suggest a method that can be applied continuously without obstructing the user's activities. For this reason, a transparent and continuous authentication mechanism provides a basis for convenient and secure re-authentication of the user.

3.5 Conclusion

This chapter has shown that current security provision seems to lack the required strength to match the respective security requirements. As presented in this chapter, biometric techniques have been identified that are applicable for deployment on mobile devices to provide continuous and transparent authentication. However, the utilisation of these techniques requires a number of considerations with regard to user acceptance, the storage of biometric information, as well as issues of performance relating to their operation in a mobile device. Furthermore, behavioural biometric authentication approaches apply a specific classifier without taking into account the nature of the applications currently being used to verify user identity.

Although several methods and systems from different perspectives have been proposed for solving the problem of mobile device security, none of the current research in this domain has investigated the risk level for each process within an application. Therefore, the next chapter presents and explores a novel taxonomy for mobile applications data in order to generalise a risk assessment model for mobile applications to identify the risk level for each process on a single application. As a result, the user's identity could be continuously verified while interacting with the mobile device by taking advantage of an intra-process security approach.

Chapter Four

A Novel Mobile Applications Data Risk Assessment Model

4 A Novel Mobile Applications Data Risk Assessment Model

4.1 Risk Assessment for Mobile Devices

Research has already been undertaken to establish how threats to mobile devices should be assessed. In their study, Ledermüller and Clarke (2011) present a mechanism to assess the risk level associated with particular apps and services. In the context of this research, applications or services that are associated with non-public information, such as emails and e-banking, would require a high level of security, whereas normal applications would require a low level of security. Consequently, each application has a particular level of risk which might be an indicator of a suitable level of security.

Similarly, Theoharidou et al. (2012) propose a risk assessment method for smartphones by identifying assets and applicable threats. The method applies user input with respect to impact valuation, coupled with statistics for calculating the likelihood of threats. The authors refined their previous work on smartphone risk assessment by proposing an approach for assessing the privacy risk of Android users (Mylonas et al., 2013). Although several methods and systems have been proposed from different perspectives for solving the problem of mobile security, none has explored the risk level for each of the processes within mobile applications.

4.2 Need for Intra-process Security

Mobile devices contain SMS, photos, calendars, notes, device settings, and apps. These data are becoming an increasingly pressing concern and the risks are high for users, such as the possibility of losing sensitive data. In addition, as stated previously, the current point-of-entry authentication mechanisms consider all applications on a mobile device to have the same level of importance and maintain a single level of security for all applications, thus not applying any further access control rules (Clarke et al., 2009). However, different applications require different security provision; for instance, a bank account requires a different level of protection compared with an SMS message. In order to access a specific service, each application needs a definite level of authentication applied in an independent manner. In particular, a high level of protection would be mapped to the riskier operations and a lower level of protection assigned to those that are less risky. Although Clarke et al. (2009) argue that the level of security within an application is likely to change during the process, they only address the issue of inter-process security by establishing appropriate levels of security for each application, rather than for the whole mobile device.

Each application has different processes, which have an impact on data and involve different levels of risk. For instance, the unauthorised disclosure of mobile applications data has the potential to lead to a number of undesirable consequences for the user. A simple example is given in Figure 4-1, which illustrates this notion in the procedure of checking the balance of a bank account without logging in. In this example, the HSBC Mobile Banking App allows the user to log on quickly and easily through the Fast Balance feature, by simply swiping

downwards on the HSBC Mobile Banking App home screen to view the balance (HSBC, 2016). This process could, however, affect confidentiality and user privacy if an impostor reads them. On the other hand, no additional risk exists for some of the processes on the HSBC Mobile Banking App, such as reading about offers, finding an HSBC branch, reading about products/services, and contacting the bank, as illustrated in Figure 4-1. The process contains public data and there is, therefore, no impact on the user if someone accesses these services. Furthermore, the level of risk will change within the mobile application and will be different from one user's perspective to another, such as the processes for reading balances and transactions.

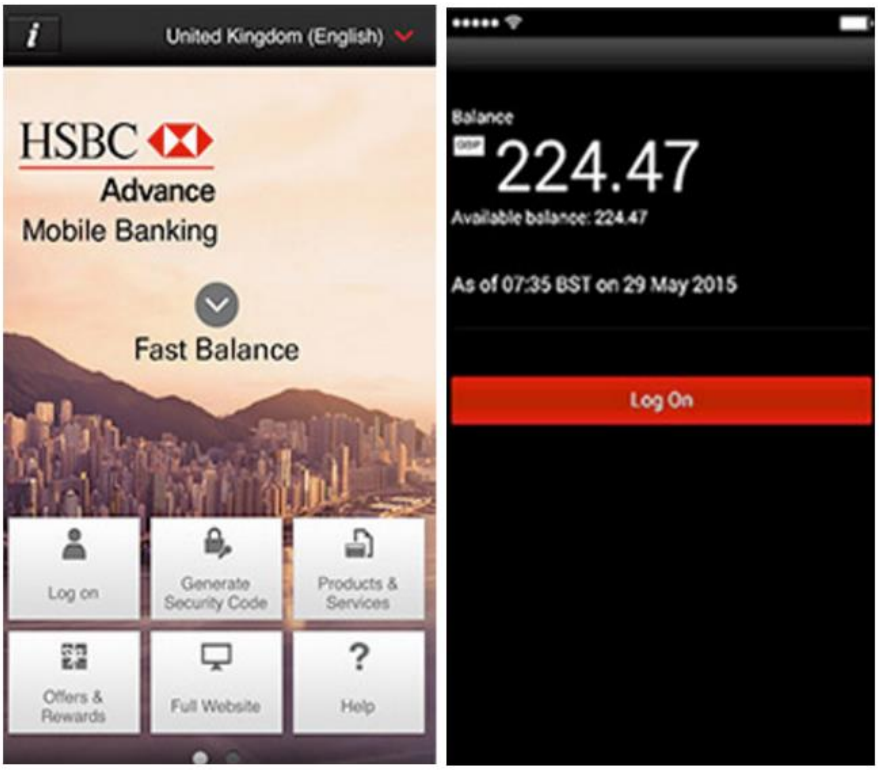


Figure 4-1: Fast Balance feature

In the Facebook mobile application, for instance, there are different processes which have an impact on data and involve different levels of risk, such as posting on a wall, sharing, sending a message and adding a photo/link. More specifically, different processes operate on the same application with different social risks, thus there is no single risk when using the Facebook application. As a result, different levels of security controls should be applied to data based on risk level in order to deny unauthorised access to the content of the application. The diagram below in Figure 4-2 indicates the threat derived from each process and the different level of risk for the various application processes. In this figure, the risk level for each process has been selected randomly to show the concept as an example.

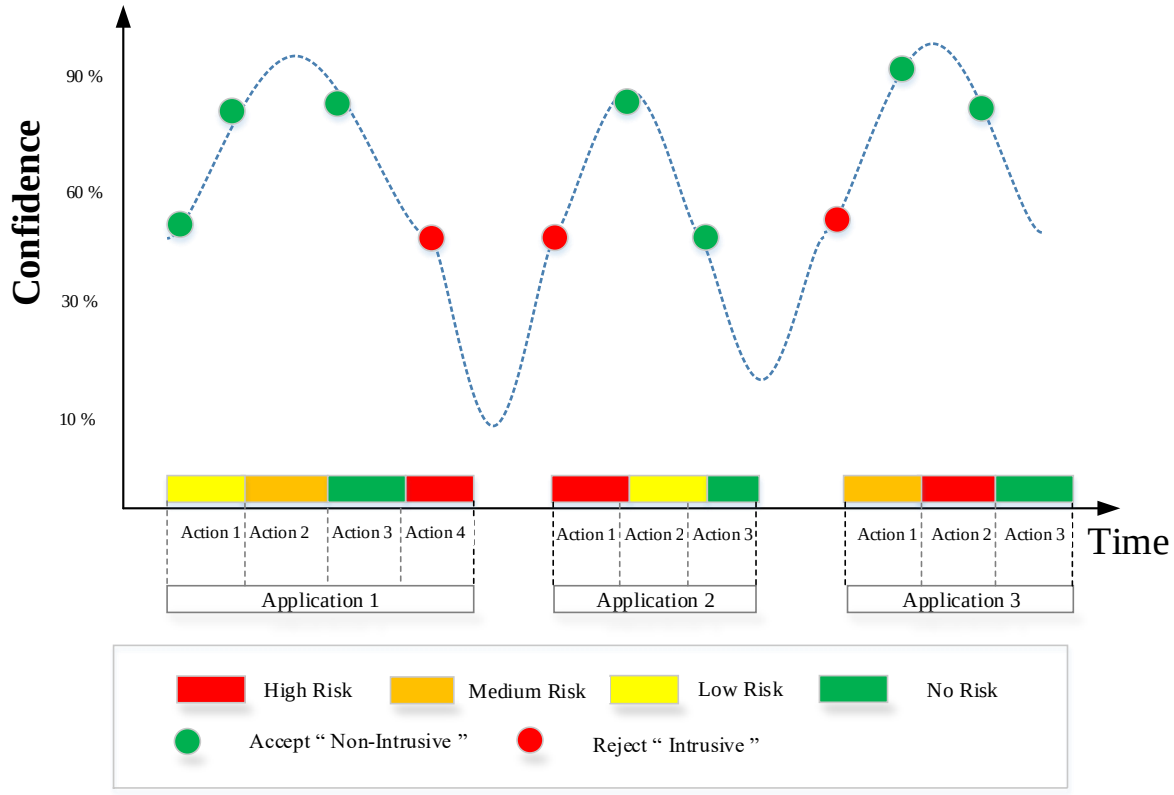


Figure 4-2: Confidence and risk action processes timeline examples

In comparison, reading news, looking at weather forecasts, watching BBC News and listening to BBC Radio 5 using the BBC mobile application are considered general data and there will be no impact on the user, just as when searching on Amazon, watching YouTube or using Google Maps. Therefore, there is no risk from accessing these services. The security implications actually start when the user is sharing public data if these data are not correct. Generally, it can be appreciated that each process on each application has a particular level of risk, which might be a feature for defining a suitable level of security by enabling *intra*-process security that would permit a far more robust approach to ensuring commensurate authenticity of the user.

It is important to ensure that the right person is allowed to access the right information at the right time. Any threat to data (i.e., action) may lead to a number of undesirable consequences, such as embarrassment, financial loss, threat to personal safety, and breach of personal privacy or commercial confidentiality (Davey, 1991). It is, therefore, important to classify data in order to strengthen the control of those data and apply risk analysis to each process. Furthermore, determining the importance of a system could be achieved by conducting risk analysis. It is also necessary to understand the nature of the risk to which the data could be exposed in order to apply the appropriate protection.

There are several and widely deployed models used for evaluating security risk such as, National Institute of Standards and Technology (NIST), CCTA Risk Analysis and Management Method (CRAMM), the ISO/IEC 27005 for Information security risk management, Operationally Critically Threat, Asset and Vulnerability Evaluation (OCTAVE), Control Objectives for Information and related Technology

(COBIT), and MEthod for Harmonized Analysis of Risk (MEHARI) (ENISA 2006; Gritzalis et al, 2018). Each one of these approaches has a different technique to assess information security risks.

•NIST SP 800-30 is a risk management guide for information technology systems which describes the risk management process based on three phases (NIST, 2012). The first phase of this method contains nine steps which would increase the complexity and the time (Gritzalis et al., 2018). This method mainly uses a scale with values Low, Medium, and High to evaluate risk (NIST, 2012). NIST SP 800-30 risk assessment model focuses on the importance of the vulnerability assessment and might be used in any kind of organization, business branch or industry area (Sepczuk and Kotulski, 2018).

•CRAMM was created in 1987 by the Central Computer and Telecommunications Agency (CCTA) subsumed in 2000 into the Office of Government Commerce (OGC) of the UK government in order to provide security evaluation of information systems in government departments. Later, CRAMM provides a commercial tool to the public through Insight Consulting (Wangen et al., 2017). The CRAMM method consists of three stages, each supported by objective questionnaires and guidelines (Shoniregun, 2006). To calculate the risk of each asset group, CRAMM uses predefined tables and comparing the value of assets, the impact and levels of threats and vulnerabilities (Gritzalis et al., 2018). In addition, CRAMM gives guidelines for each criterion on how to measure the described consequence on a scale from 1 to 10. Furthermore, CRAMM calculates the levels of threat to assets on a five-point scale of “Very Low, Low, Medium, High or Very High”, as well as levels of vulnerability to threats on a scale of “Low, Medium or High”. Each

possible answer carries a numerical weighting which reflects the relative importance of its contribution to the total threat or vulnerability rating. As each questionnaire is completed, CRAMM sums the weighting and categorises the total as “High, Medium, or Low”. CRAAM emphasis on data itself.

•OCTAVE was developed by the Software Engineering Institute of the Carnegie Mellon University’s computer emergency response team in order to define a risk-based strategic assessment and planning technique to understand and address its information security risks (Sepczuk and Kotulski, 2018). OCTAVE is a self-directed approach which that in turn meaning employees from an organization might be able to set the organization’s security strategy without the need for security experts (ENISA, 2006). This method has three main phases, organizational view, technological view and strategy and plan development.

•COBIT was created by international professional association ISACA for information technology management and IT governance to make better decisions regarding their information and technology assets by implementation a set of controls over information technology and organises them around a logical framework of IT-related processes and enablers (Haes and Grembergen, 2016). This method contains four areas namely plan and organize; acquire and implement; deliver and support; and monitor and evaluate. In addition, there are 34 processes in line with the four areas.

•ISO/ IEC 27005 comprises information security standards which published jointly by the International Organization for Standardization (ISO) and the International

Electrotechnical Commission (IEC) to provides best practice recommendations on information security management.

•MEHARI was developed in 1996 in order to assist operating managers, CISO, CIO, and risk manager o manage the security of Information and IT resources and to thereby reducing the associated risks. In order to achieve a continuous improvement cycle, MEHARI work on a list of vulnerability control points and an accurate monitoring process. In addition, MAGERIT can use either qualitative or quantitative calculations of risk and conducts risk calculation via predefined tables or algorithmic analysis (Gritzalis et al., 2018).

In the earlier literature review, studies have used CRAMM in the context of other applications. For instance, Josang et al. (2004) describe a method for belief-based risk analysis based on the approach used in CRAMM by quantifying threats and vulnerabilities as beliefs and impact costs in dollars and cents. In addition, Maglogiannis and Zafiropoulos (2006) present a modeling approach for achieving a risk analysis study of networked healthcare information systems based on CRAMM. Afterwards, Maglogiannis et al. (2006) suggest an improved methodology by combining basic features of the CRAMM risk analysis method with the Bayesian Network modeling technique in order to identify assets, threats and vulnerabilities of patient systems. On the other hand, El Fray (2012) presents a comparative study of a developed new formal mathematical model of risk assessment (FoMRA) with expert methods of risk assessment in the information systems (MEHARI and CRAMM). Furthermore, Ghazouani et al. (2014) propose a practical approach with a mathematical formulation of risk by analysing the

studied methodology of CRAMM, NIST SP 800-30, OCTAVE, and ISO 27005 to propose a qualitative approach for assessing information security risks.

Moreover, acknowledging that while NIST SP 800-30 is a more recent approach and still being maintained/revised, it has a different focus that research felt was less suited to research needs. Therefore, it seemed a reasonable basis to use in this case as well rather than creating a different approach for the sake of it. More specifically, the proposed risk method is only adopting the impact rating approach (i.e. rather its approach to impact classification in relation to data) and not using the entire CRAMM aspects.

Impact types represent the way in which data are affected if Confidentiality, Integrity and Availability (CIA) security is breached. In CRAMM, there are four main types of impact (Davey, 1991):

- Disclosure: Unauthorised disclosure of data.
- Modification: Accidental or deliberate alteration of data.
- Denial: Denial of access to data.
- Destruction: Destruction of the system or data.

4.3 Taxonomy of Mobile Applications Data

To the best of this author's knowledge, the risk for each process within the application has not been investigated. The first step to take in exploring risk is to propose a taxonomy of mobile applications data. In this context, destruction impact type not fit due to it related to the total loss of data rather than the partial loss of some records and still the same risk of modification impact. Likewise,

denial would be work with a higher level for application instead of a specific process because the application has not stopped in practical way. Int this context, availability was not used due to there is possibility to access the mobile application and our approach behind this step. In this methodology, there were three types of mobile applications data taxonomy, as shown in Figure 4-3:

1. Based on impact type (disclosure, modification).
2. Based on information type (public, non-public).
3. Based on impact consequences.

The impact consequences have been adopted from CRAMM (Davey, 1991) as follows:

- *Embarrassment*: “thing causing feelings of embarrassment for a person”.
- *Financial loss*: “loss of money”.
- *Breach of personal privacy*: “when there is unauthorised access or disclosure of personal information”.
- *Breach of commercial confidentiality*: “business information between the user and organisation”.
- *Legal liability*: “concerns both civil law and criminal law when the user is financially and legally responsible for something”.
- *Threat to personal safety*: “a situation which may be in the form of harassment, an assault, or sexual assault”.
- *Disruption*: “inconvenience and annoyance”.

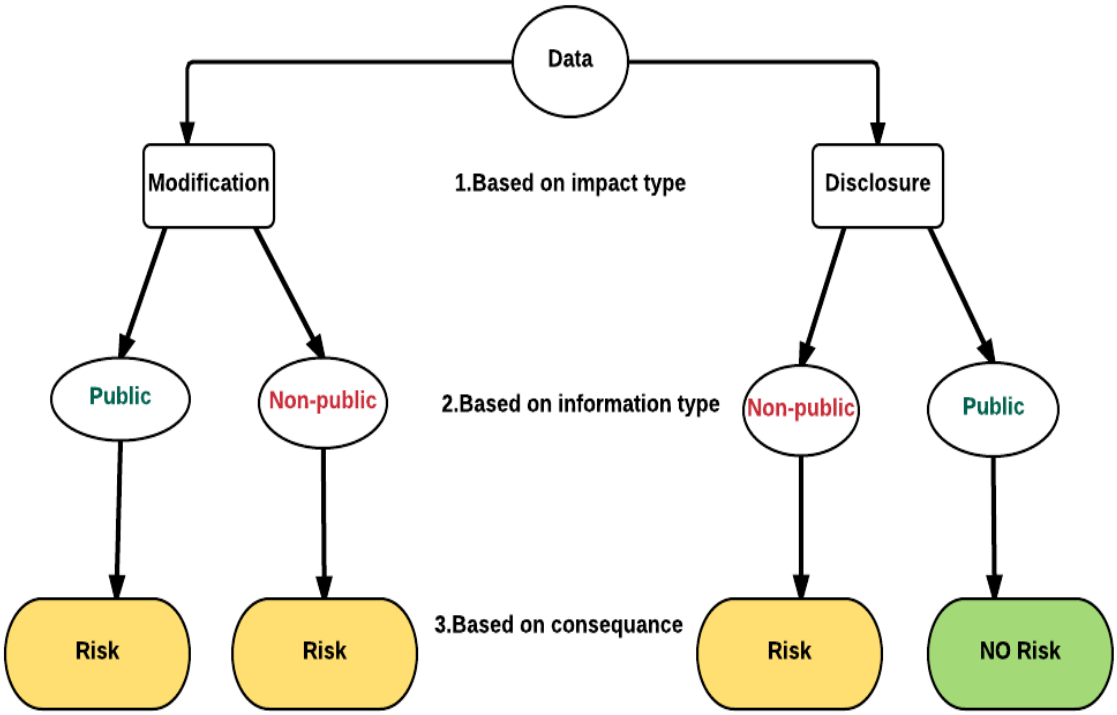


Figure 4-3: Taxonomy of mobile applications data

1- Based on impact type

Data sensitivity has been considered in terms of the potential impact in the event of a breach of security that may result from lack of confidentiality, integrity and availability. These factors are thus the basis for classifying data. In this stage, only two impact types have been identified based on CRAMM: disclosure and modification, as shown in Table 4-1. In this context, destruction impact type does not fit, as it is related to the total loss of data rather than the partial loss of some records, but still has the same risk of modification impact. Likewise, denial would work with a higher level for an application instead of a specific process because the application has not been stopped in a practical sense.

2- Based on information type

These data can be classified based on the type of information (public or non-public). In the public data type of disclosure impact, there is no need to require verification of the user's identity due to there being no risk or impact on the owner's privacy, such as when reading the news, accessing weather forecasts or opening maps. As a result, no controls are required to protect the confidentiality of public data when a non-owner tries to access a public application in terms of a disclosure impact. However, if public data were modified incorrectly, this could have an impact in terms of disruption or personal safety if an incorrect decision is made based on the modified public data and might cause embarrassment for an organisation. In contrast, loss, misuse, modification, or unauthorised access to non-public data type can adversely affect an individual and may cause financial loss, as well as the leak of personal information such as credit card numbers, bank account details, and health data. As a result, the highest level of security control should be applied to sensitive data in order to deny unauthorised access to the content of the application.

3- Based on impact consequences

Definition	Security breach
Unauthorised *disclosure* may result in *embarrassment.*	Confidentiality
Unauthorised *disclosure* may result in *legal liability*.	Confidentiality

Definition	Security breach
Unauthorised *disclosure* may have an impact *on personal privacy.*	Confidentiality
Unauthorised *disclosure* may result in *data corruption.*	Confidentiality
Unauthorised *disclosure* may result in *financial loss.*	Confidentiality, Integrity
Unauthorised *disclosure* may result in a breach of commercial confidentiality.	Confidentiality
Unauthorised *disclosure* may threaten *personal safety.*	Confidentiality
Unauthorised *modification* may result in *embarrassment.*	Confidentiality, Integrity
Unauthorised *modification* may result in *legal liability.*	Integrity
Unauthorised *modification* may have an impact on *personal privacy.*	Integrity
Unauthorised *modification* may result in *financial loss.*	Integrity
Unauthorised *modification* may result in *data corruption.*	Integrity
Unauthorised *modification* may result in a breach of *commercial confidentiality.*	Confidentiality
Unauthorised *modification* may result in *disruption.*	Integrity

Definition	Security breach
Unauthorised *modification* may threaten *personal safety.*	Confidentiality

Table 4-1: Definition of types of impact on data and consequences

In this research project, the 10 most popular mobile categories were selected and the most-used application for each category was chosen based upon Google Play ranking (Nielsen, 2015). Table 4-2 presents a more detailed analysis of these applications and considers the processes that a mobile user performs most regularly on each one. More specifically, there are different processes that operate on the same data and might pose different levels of social risk. This analysis was done by investigation the entire function inside the selected application. For instance, adding photos on Facebook might be considered a sensitive process that affects the user's privacy, while reading the text on the BBC News application does not. Based on the first level of the novel proposed taxonomy, these processes can be classified into public or non-public, in order to identify the impact consequence at the second level of the proposed taxonomy. After the analysis of user actions (processes) on each application, a total of 115 actions were identified (97 non-public and 18 public actions). The results show that 81% of the actions involve non-public data and 19% public data. Therefore, the majority of actions involve sensitive data, which might affect user privacy and confidentiality based on the second level of the taxonomy. The results suggest there is a need to verify the user's identity after point-of-entry authentication.

Traditionally, all processes within a typical mobile application are assumed to have the same level of risk. However, the analysis carried out for this thesis

suggests that this assumption is not always true. For instance, in the HSBC Mobile Banking application, paying bills and reading about products/services are not considered by the researcher having the same level of risk. Furthermore, sharing a video in a YouTube application does not carry the same level of risk as watching on a YouTube process. Accordingly, it is worth noting that the different processes on a single application have different levels of risk and thus there is clearly a different level of risk within the application.

App	No.	User action	Information type	Impact type
Facebook	1	Search on Facebook	Public	No Impact
	2	Read news feed	Non-public	Disclosure
	3	Read user profile	Non-public	Disclosure
	4	Post on a wall	Non-public	Disclosure, Modification
	5	Add photo/link	Non-public	Disclosure, Modification
	6	Tag friends/check in	Non-public	Disclosure
	7	Like	Non-public	Disclosure, Modification
	8	Comment	Non-public	Disclosure, Modification
	9	Share	Non-public	Disclosure
	10	Read notifications	Non-public	Disclosure
	11	Send message	Non-public	Disclosure, Modification
	12	Read message	Non-public	Disclosure
	13	Delete message	Non-public	Disclosure, Modification
	14	Join group	Non-public	Modification
	15	Voice call/video call	Non-public	Modification
	16	Change settings	Non-public	Modification
	17	Update information	Non-public	Disclosure, Modification
	18	Add friend	Non-public	Modification
	19	Remove friend	Non-public	Modification
YouTube	1	Search on YouTube	Public	No Impact
	2	Watch on YouTube	Public	No Impact
	3	Upload	Non-public	Modification
	4	Share	Non-public	Disclosure
	5	Like/dislike	Non-public	Disclosure, Modification
	6	Add a comment	Non-public	Disclosure, Modification

App	No.	User action	Information type	Impact type
	7	Search history	Non-public	Disclosure
	8	Add to watch later	Non-public	Modification
	9	Subscribe	Non-public	Modification
	10	Unsubscribe	Non-public	Modification
	11	Read subscriptions	Non-public	Disclosure
	12	Read created playlists	Non-public	Disclosure
	13	Create a new playlist	Non-public	Modification
	14	Browse channels	Non-public	Disclosure
Gmail	1	Search on Gmail	Non-public	Disclosure
	2	Send an email	Non-public	Disclosure, Modification
	3	Read a new email	Non-public	Disclosure
	4	Read an old email	Non-public	Disclosure
	5	Reply to/forward	Non-public	Disclosure, Modification
	6	Delete an email	Non-public	Disclosure, Modification
	7	Chat on Gmail	Non-public	Disclosure, Modification
	8	Make a call	Non-public	Disclosure, Modification
	9	Change settings	Non-public	Modification
	10	Read user's contact	Non-public	Disclosure
	11	Read sent mail	Non-public	Disclosure
	12	Read important email	Non-public	Disclosure
	13	Read user's note	Non-public	Disclosure
Google Drive	1	Search on drive	Non-public	Disclosure
	2	Read file	Non-public	Disclosure
	3	Share file	Non-public	Disclosure
	4	Delete file	Non-public	Disclosure, Modification
	5	Upload file	Non-public	Modification
	6	Download drive	Non-public	Disclosure
	7	Show recent file	Non-public	Disclosure
	8	Upgrade storage	Non-public	Modification
	9	Change settings	Non-public	Modification

Table 4-2: Mobile applications analysis

Figure 4-4 shows that Gmail, Google Drive and Google Photos are considered sensitive applications because 100% of what they include is sensitive personal user data. On the other hand, BBC News tends not to be a sensitive application

because the majority of its processes (83%) contain public data, such as reading the news and searching on BBC News. In the absence of a potential impact, no risk is considered to exist. However, if an adversary maliciously manipulates someone else's public data and shares or publishes them publicly, this could have a negative impact on the individual's personal safety or cause embarrassment for an organisation if an incorrect decision is made based on the manipulated data. Furthermore, Google Maps contains only 36% public data, such as searching on Google Maps, getting directions, and showing traffic. Similarly, only 13% of the Gumtree application and 7% of the Amazon app are considered to be public data.

Interestingly, HSBC Mobile Banking contains about 33% public data, such as reading about products, finding an HSBC branch and reading about offers, while there are about 67% non-public processes which need more protection. However, the majority of user actions on Facebook (95%) are deemed risky processes, such as posting on the wall, sharing, and adding photos. YouTube is also classified as a sensitive application because nearly 86% of its process involves non-public data. However, the user could use the YouTube application to search for or watch a video and, therefore, such processes are considered to involve public data, which represent only 14% of YouTube processes.

Considering the aforementioned findings, this investigation demonstrates that there is no single risk to using a given application, since the risk changes within the application from one process to another. More specifically, the unauthorised disclosure or modification of mobile applications data has the potential to lead to a number of undesirable consequences for the user.

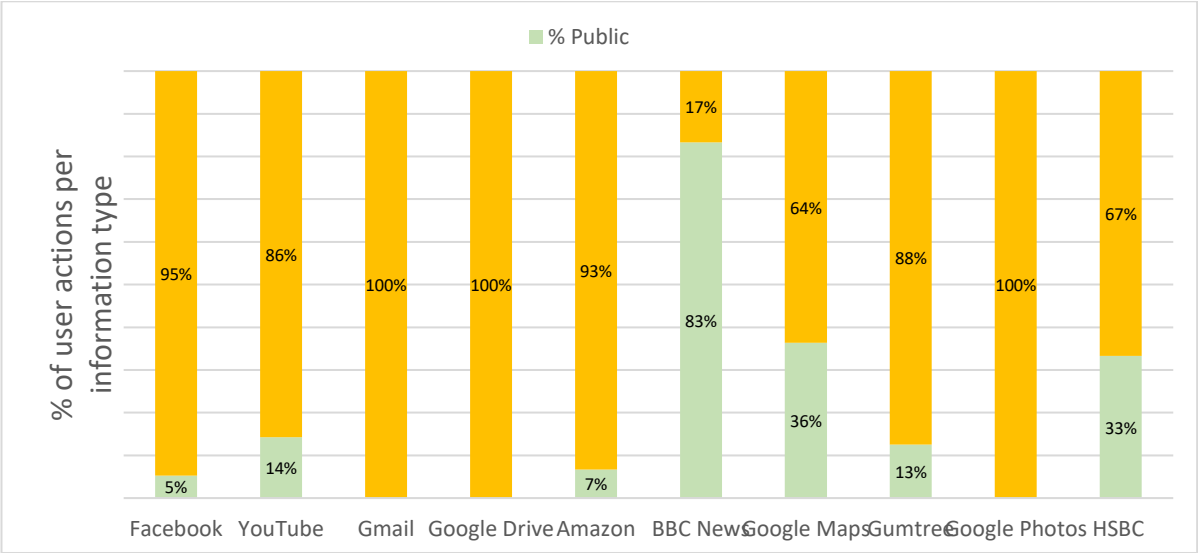


Figure 4-4. Percentages of actions involving public and non-public data

4.4 Generic Risk Assessment Model for Mobile Applications

When exploring the consequences of a security breach, it can be seen that the level of risk changes within an application (intra-process). More specifically, different processes operate on the same application with different social risks, thereby there is no single risk for a single application. Furthermore, there is a degree of complexity and a number of aspects on a personal level that need to be calculated from one person to another due to differences in culture and education types between users.

Types of impacts are a relevant set of consequences worthy of consideration in the context of mobile apps. For example, loss, modification, or unauthorised access to non-public data can adversely affect an individual and may cause financial loss from the user's bank account or the leaking of personal information, such as credit card numbers, bank account details, and health data. Similarly, unauthorised disclosure, such as access to images and messages, may result in

embarrassment if shared by others. More specifically, different processes operate on the same application, with different levels of social risk involved, so there is no single risk for a single application. Furthermore, there are complex personal aspects that need to be calculated: users may belong to different cultures and have received different levels of education. Traditionally, risk calculation is related to a combination of impact and likelihood (i.e., probability of occurrence), as in the following equation:

Risk = Impact consequence x likelihood *(1)*

Each specific impact type has its own specific set of consequences. Each of these consequences could be assessed using a 1-10 rating scale, based on CRAMM, but this would make the methodology far too complex for the user. For the sake of simplicity, the impact consequences are rated at different levels (low impact, medium impact, and high impact), which provides a component of the measure of risk. Furthermore, it is possible to find disclosure and modification impact types on specific data, such as posting on a wall in a Facebook application. Thus, this research uses a 3-dimensional risk matrix containing the impact type (disclosure or modification or both), information type (public or non-public) and impact consequences (embarrassment, financial loss, data corruption, disruption, legal liability, threat to personal safety, breach of commercial confidentiality, and breach of personal privacy). This risk model is applied to each action data on each application in order to investigate the risk.

To calculate the risk level based on the suggested risk model, there is a need to identify a process value (the degree of importance) and the maximum

consequences of this action. In addition, the users are not in a position to make meaningful/informed decisions about the importance of the action to them and, therefore, their perceptions are likely to be invalid. In this context, the process value (P) is the level of importance of the action:

0: not important
1: low importance
2: medium importance
3: high importance
4: very important

$$Risk=Process\ value,max\{d(c\_max),m(c\_max)\} \quad (2)$$

Where d is impact disclosure; m is impact modification, and c is consequence.

The process value is identified on the basis of the following equation:

$$Process\ Value = Application\ Rank \times Process\ Weight \quad (3)$$

In Table 4-3, the application categories have been collected on the basis of the Google Play classification of application type and ranked on a scale from 1 to 3. The intention of this scale is to show the diversity between the levels of importance of the actions within applications regarding the user's privacy and in order to attribute sensitivity levels. Towards this goal, three numbers were used to determine the level of importance of user data privacy: '1' means the application category is not important because it does not contain any user data (such as BBC Weather); '2' means a category of medium importance because it contains user data; and '3' is an application category of high importance because it includes sensitive user data and any possible action on these data might

concern, for example, the user's bank details. These application categories have been predefined to illustrate the idea behind the suggested risk model:

*Risk = Max {Impact **Disclosure** (Max consequence), Impact **Modification** (Max consequence)}*

To assess the level of potential impact of each process (i.e., threat), the 'worst-case scenario' principle was adopted by answering the following questions (Theoharidou et al., 2012), the answers to which are used to calculate the impact for each process:

- Which are the worst consequences if your data are disclosed to unauthorised users?
- Which are the worst consequences if your data are modified or damaged?

Category	Rank	Example	Category	Rank	Example
Business	2	PDF Reader	Shopping	3	Amazon
Books and Reference	2	Kindle	Social	3	Facebook
Comics	1	Draw Cartoons	Sports	1	Sky Sports
Communication	3	WhatsApp	Medical	2	myGP
Education	2	TED	Music and Audio	1	SoundCloud
Entertainment	2	BBC iPlayer	News and Magazines	1	BBC News
Finance	3	HSBC Bank	Personalisation	2	File Manager
Food and Drink	2	Just Eat	Photography	3	Google Photos
Health and Fitness	1	Google Fit	Productivity	3	Google Drive
Games	1	Pokémon	Lifestyle	2	IKEA Cat.
Maps	2	Google Maps	Tools	1	Alarm Clock
Weather	1	BBC Weather	Travel and Local	2	Booking

Table 4-3 : Application categories ranking

The process weight is given on the basis of the process type rankings shown in Table 4-4. These numbers are for illustration purposes and have been predefined by experts. For example, reading news is considered a very low-risk action due to this involving public data (disclosure public type), whereas sharing a user photo might be a high-risk action (modification non-public type).

Process Type	Process Weight
Disclosure Public (DP)	0
Modification Public (MP)	1
Disclosure Non-public (DN)	2
Modification Non-public (MN)	2

Table 4-4: Process weighting

Furthermore, risk levels might increase differently in relation to various consequences and a weight for each impact consequence is given, as shown in Table 4-5. In this context, the weight value will be one of three (0, 1, and 2) to differentiate between impact consequences. Embarrassment, for example, is higher than financial loss in the process type “disclosure non-public”. The weight values for disclosure public will be 0 for all consequences because there is no impact effect on the user. Therefore, there is no risk involved in the disclosure public type. Whereas, the weight value for modification non-public is 2 for all consequences. The reason for rating all consequences as 2 is that disclosure non-public happens before the modification step and, therefore, the rate for all

consequences should be higher than the rate for all consequences in disclosure non-public type. In the “modification public” type, the weight values differ from one impact consequence to another. In practice, at the point of installation or at any time subsequently, users have the opportunity/ability to set their own preferred rank based on how important they believe it to be and these weights have been predefined by experts to illustrate the idea of the suggested risk model.

In Table 4-5, due to space limitations, the following notation is used to show the impact consequences:

- E = Embarrassment
- F = Financial loss
- PP = Breach of personal privacy
- CC = Breach of commercial confidentiality
- LL = Legal liability
- PS =Threat to personal safety
- D = Disruption

Each consequence has three values:

- 0 = Low
- 1 = Medium
- 2 = High

The resulting risk is measured on a scale from 0 to 5 as per the following criteria:

- 0-2 = Low risk
- 3 = Medium risk
- 4-6 = High risk

PT / C	DP	DN	MN	MP
E	0	2	2	2
F	0	1	2	1
PP	0	2	2	1
L	0	1	2	1
PS	0	2	2	1
D	0	2	2	1
C	0	1	2	2

Table 4-5: Consequences weighting

Each consequence has three values (low, medium, and high) and each action or threat is mapped to at least one impact consequence. In cases where there is more than one impact consequence, the highest of the values is chosen. The resulting risk is measured on a scale from 0 to 6 according to the following criteria: 0 = No risk; 1 or 2 = low risk; 3 or 4 = medium risk; and 5 or 6 = high risk. To assess the level of potential impact of each process (i.e., threat), the 'worst-case scenario' principle has been adopted to answer the following question (Mylonas, 2013), the answer to which is used to calculate the impact for each process. The question is: Which are the worst consequences if <your data> are disclosed to / modified by unauthorised users?

Table 4-6 shows the results of the multiplications in two scenarios based on impact consequences, at weights 1 and 2.

		Impact Consequences Weighting					
		When impact consequence weight = 1			When impact consequence weight = 2		
		L	M	H	L	M	H
Process Value	0	0	0	0	0	0	0
	1	1	2	3	2	4	6
	2	2	3	4	4	6	6
	3	3	4	5	6	6	6
	4	4	5	6	6	6	6

Table 4-6: Impact consequences weighting

Finally, Table 4-7 shows the simplified risk matrix.

		Impact Consequences Weighting					
		When impact consequence weight = 1			When impact consequence weight = 2		
		L	M	H	L	M	H
Process Value	0	No Risk	No Risk	No Risk	No Risk	No Risk	No Risk
	1	Low	Low	Medium	Low	Medium	High
	2	Low	Medium	Medium	Medium	High	High
	3	Medium	Medium	High	High	High	High
	4	Medium	High	High	High	High	High

Table 4-7: Simplified risk matrix

Let us assume cs is a vector that represents the consequence selection of the impact of the consequence c, in which every element in cs is either 0, meaning no impact, or 1 has impact, and cs has at most a single 1: $cs \in \{0,1\}^{(m\times o)}$

The process risk has been assessed by calculating the maximum vector component-wise multiplication vector outcome, denoted by ⊗, between ⟦RM⟧

_adjusted and cs row given by the process and cs vector.

$$\text{Process Risk} = MAX([RM_E(Process\ value)|RM_F(Process\ value)|\cdots|RM_D(Process\ value)] \otimes cs) \quad (6)$$

Finally, the result of the computation is a scalar value in T. The pseudocode of the mobile applications data risk assessment model is illustrated below and is summarised in Algorithm 1, as follows.

Algorithm 1. Mobile applications data risk assessment model

```
Input:  Application Rank; Process Type; Consequence selection
Output: Process Risk
1: if Process Type = "Disclosure Non-public":
2:    then Process Weight= 2 and Consequences Weight = (1, 0.5, 1, 0.5, 1, 1,
0.5)
3: else if Process Type = "Modification Non-public":
4:   then Process Weight= 2 and Consequences Weight = (1, 1, 1, 1, 1, 1, 1)
5: else if Process Type = "Modification Public":
6:   then Process Weight= 1 and Consequences Weight = (1, 0.5, 0.5,0.5,0.5, 0.5,
1)
7: else Process Risk = 0
8: end if
9: Process Value = Application Rank * Process Weight
10: New Risk Matrix [] = Ceil (Risk Matrix [] * Consequences Weight)
11: Process Risk = Max (New Risk Matrix [Process Value] * Consequence selection)
```

Table 4-8 provides a demonstration of the MORI assessment method with different user actions within the application at all possible impact consequence

weight scenarios. For further clarification, the following numbers have been calculated based on equations 2 and 3 from the above analysis to show the proposed risk model approach. In addition, these examples might help the user to understand the diversity level of the risk and thereby apply the appropriate level of an authentication method in a usable and secure manner.

App	User action	Process Type	App Rank	Process Weight	Process Value	Risk
HSBC	Make transfer	MN	3	2	6 ≈ 4	6
	Read offers	DP	3	0	0	0
	Find HSBC branch	DP	3	0	0	0
	Read transactions	DN	3	2	4	4
	Read balances	DN	3	2	4	4
Weather	Forecast weather	DP	1	0	0	0
	Share with	MP	1	1	1	1
	Change setting	DN	1	2	2	3
Facebook	Search	DP	3	0	0	0
	Read news feed	DN	3	2	4	4
	Share	MP	3	1	3	6
	Read user profile	DN	3	2	4	5
	Post on a wall	MN	3	2	4	6
	Add photo/link	MN	3	2	4	6
BBC	Search	DP	1	0	0	0
	Watch BBC News	DP	1	0	0	0
	Share	MP	1	1	1	3
YouTube	Search on	DP	2	0	0	0
	Watch on YouTube	DP	2	0	0	0
	Upload	MN	2	2	4	5
	Add a comment	MN	2	2	4	5
	Search history	DN	2	2	4	4
	Read subscriptions	DN	2	2	4	4

SMS	Send a message	DN	3	2	4	6
	Read a message	DN	3	2	4	5
	Delete a message	MN	3	2	4	6
Calling	Make a call	DN	3	2	4	6
	Receive a call	DN	3	2	4	4
	Read a history call	DN	3	2	4	4
WhatsApp	Chat	DN	3	2	4	5
	Send a photo	DN	3	2	4	6
	Share a location	DN	3	2	4	5
	Share a document	DN	3	2	4	5
Email	Read an email	DN	3	2	4	5
	Send an email	DN	3	2	4	6
	Delete an email	MN	3	2	4	6

Table 4-8: Risk assessment examples

To conclude, this chapter has introduced a new risk assessment model for mobile applications data, called MORI (Mobile Risk), which determines the risk level for each process on a single application. In particular, the MORI model depends upon the value of a user action and the worst consequences if user data are disclosed to unauthorised users or modified without permission. Finally, this model has introduced a risk matrix which might help move the access control system from the application level to the intra-process application level, based on the risk for the user action being performed on these processes. The findings demonstrate that this model has introduced a risk matrix which helps to move the access control system from the application level to the intra-process application level, based on the risk for the user action being performed on these processes. In the future, this risk matrix could assist research activities that investigate the risks within an application. Future research could focus upon suggesting and

applying a usable approach to accessing mobile phones by considering the risk level for each sensitive process and introducing the level of authentication beyond the point-of-entry approach. Furthermore, future work could focus on usability and how the user interacts with the proposed risk matrix to ensure that it best fits the individual's favourite settings.

Chapter Five

Investigation of Transparent User Authentication for Mobile Applications

5 Investigation of Transparent User Authentication for Mobile Applications

5.1 Introduction

The previous chapter proposed a taxonomy for mobile applications data and introduced a novel mobile applications data risk assessment model to understand the risk involved within an application (intra-process security). Chapter 4 demonstrates that there is no single risk to using a given application since the risk changes within the application from one process to another. This study has also indicated the need to move an access control system from a position on an application to within the application based on the risk level for each action, which means there is a clear need to collect and model real-world data. This, in turn, indicates the need to investigate the relationship between the transparent capture of biometric samples and the resulting access control decisions (Clarke et al., 2009; Chuang et al., 2018). As such, this research aims to better understand and investigate the potential for applying a transparent authentication system to intra-process security. This system would, in turn, enable control of the overall authentication process and thus a continuous and non-intrusive authentication approach.

This chapter presents the methodical approach used for the data collection and experimental methodologies for the proposed biometric transparent authentication system at the intra- and inter-process access levels and then

presents the experimental results and analysis for three experiments. The three experiments, and the main aim of each, are as follows:

- **Experiment 1 - A biometric transparent authentication system at the intra- and inter-process levels:** The average rate of intrusive authentication requests was computed and demonstrated for both the intra-process (within the application) and inter-process (application access only) levels in this experiment. The main aim of this experiment was to test the impact of the inter- and intra-process on the overall transparent user authentication approach for mobile applications by including the application access with other actions within the application for 76 participants and then to apply the same concept for three types of usage (low, medium and high).
- **Experiment 2 - A biometric transparent authentication system at the intra-process level:** A set of experiments was conducted to provide further insight into whether applying a transparent authentication system to an intra-process would enhance security and usability. The experiments were applied to each user file to compute the average intrusive authentication requests within the application only for 76 participants and the same concept was then applied to three types of usage (low, medium and high). The primary aim of considering participant categories was to gain greater insight into how low usage would affect the total average intrusive authentication requests for the entire dataset.

- **Experiment 3 - A biometric transparent authentication system at the inter-process level:** To test the research concept, it was deemed useful to conduct an evaluation using the same real-world dataset. To achieve this goal, the average intrusive authentication requests were calculated and presented for the inter-process (application access only) without taking the actions which were happening within the application into account for 76 participants. In this experiment, the same concept was also applied to three types of usage (low, medium and high).

5.2 Experimental Methodology

This section demonstrates how the data were collected and then explains the methodical scientific approach of the three experiments outlined above.

In order to investigate the feasibility of building a transparent and continuous biometric-based system, it is necessary to collect samples of genuine user interactions with their mobile devices/apps, based upon a substantive period of real-world use (noting that such samples would be based upon data that are naturally logged by apps on the devices already and so the research would not be gathering information that was not already available – it would, however, be applying it to an additional purpose). As such, it was proposed to enlist participants and collect log data from them after one month of normal device usage. It should be noted that the data were anonymous and that participation did not require the participants to do anything other than use their devices as normal. This experiment collected the sort of data that are logged routinely, such as a time stamp of the application used by the participant and the name of the

user action (read, send, etc.) but did not collect data such as passwords or messages.

The experiment was carried out on the participants' Android mobile phone. Ethical approval for this research project was obtained from the university's Research Ethics Committee (Appendix A) in order to fulfil University of Plymouth requirements. All the participants were 18 years or older and were asked to read and sign a consent form (Appendix B) and information sheet regarding data collection (Appendix C) before starting the experiment. In addition, the research and data were conducted and stored within the Centre for Security, Communications and Network Research (CSCAN) at Plymouth University (start date: February 2017; end date: July 2017). Although the study was conducted to collect app log data, no sensitive material was involved. To facilitate a meaningful analysis, at least 100 adult participants (18 years or older) were invited to participate in this metadata capture experiment. Participants took at least one month to complete their participation in the study, during which time they were simply asked to use their device as normal.

For the purpose of the data collection, a code was developed to extract log files from a backup file from the participants' devices after taking a backup after one month on the principal investigator. After one month, each participant's mobile device was connected to the main investigator's computer. Mobile backup was started by utilising Android Debug Bridge (ADB), which is a command line tool that allows communication between the connected Android device and a computer. This necessitated the participating devices having Android OS version

4.1 or above. To access iOS, there is a need to jailbreak the devices to access the log files which unlikely for the users to accept that. On the other hand, android allow to access to mobile detailed and extract data log files without the need to root. Ina addition, to protect the user privacy, ADB was used instead of asking the mobile user to download application.

The backup file was extracted and the participant's mobile phone was disconnected. Then, a code was run on SQLite to extract the log files from the extracted backup file. Next, data were generated and the information column was exported to a datasheet file (the time stamp, application name and process name) and stored in a folder called the "UserActionDataSheet". The data were then reviewed by the participant to verify that he/she agreed to share them with the investigator. Finally, the backup file was removed at the end of the experiment period. Although the study is going to collect app log data, there is no sensitive material involved in doing this by writing a code to extract all data automatically once connect the mobile device and protect the user privacy.

During this phase of the data collection, the following applications were selected and collected, as shown in Table 5-1, and a package name and database name given to each selected application. Some applications, such as Facebook, Online Mobile Banking, and Chrome, were fully encrypted and there was no way of collecting user data without compromising the user's privacy by asking the participant to root his/her device. For this reason, only 11 applications were collected in order to protect the user's privacy.

No.	Application	Package name	Database
1	Phone Call	om.sec.android.provider.logsprovider	logs
2	SMS	com.sec.android.provider.logsprovider	logs
3	Downloading	com.android.providers.downloads	downloads
4	YouTube	com.google.android.youtube	history
5	WhatsApp	com.whatsapp	msgstore
6	Browser	com.sec.android.app.sbrowser	SBrowser_Tabs
7	Google Play	com.android.vending	localappstate
8	Email	com.android.email	EmailProvider
9	Viber	com.viber.voip	viber_data; viber_messages
10	Google Photo	com.google.android.apps.photos	gphotos0_local_media
11	Camera	com.android.providers.media	external_Images
			external_video
12	Yahoo mail	com.yahoo.mobile.client.android.mail	mailsdk_messages

Table 5-1: Applications collected from users' mobile phones

Before starting the data analysis, the risk model (MORI) was used to calculate the risk level for each action and applied to the participants' data to show the diversity of the risk level for the different types of actions within each application. Table 5-2 shows the 12 selected applications for which the risk level was calculated for each user action inside the application for the final stage of the risk calculation. The action risk level was identified, as shown in Table 5-2, using the following range: high risk (6 or 5), medium risk (4 or 3), low risk (2 or 1) and no risk (0). As shown in Table 5-2, on a single mobile application, different processes operate on the same data with different social risks based on the user action. For instance, the WhatsApp application contains different levels of action risk: sending a text

message is considered high risk (6), whereas receiving an audio message is considered medium risk (4) and receiving a free call (voice/video) is considered low risk (2). Finally, each user's data were updated after applying the risk model and stored in an individual text file to calculate the biometric and then identify the identity confidence level.

No.	Action Name	Application	App Risk	Action Risk
1	Make a call	Phone Call	3	6
2	Receive a call	Phone Call	3	4
3	Read an SMS message	SMS	3	5
4	Send an SMS message	SMS	3	6
5	Download a file	Downloading	2	3
6	Search on YouTube	YouTube	1	0
7	Receive a text message	WhatsApp	3	5
8	Receive an image message	WhatsApp	3	3
9	Receive an audio message	WhatsApp	3	3
10	Receive a video message	WhatsApp	3	3
11	Receive a contact card	WhatsApp	3	3
12	Receive a location	WhatsApp	3	4
13	Receive a free call (voice/video)	WhatsApp	3	2
14	Receive a PDF file	WhatsApp	3	4
15	Send a text message	WhatsApp	3	6
16	Send an image message	WhatsApp	3	6
17	Send an audio message	WhatsApp	3	6
18	Send a video message	WhatsApp	3	6
19	Send a contact card	WhatsApp	3	4
20	Send a location	WhatsApp	3	6
21	Make a free call (voice/video)	WhatsApp	3	5
22	Send a PDF file	WhatsApp	3	5
23	Search	Browser	1	0
24	Watch a video	Browser	1	1
25	Download an app	Google Play	2	4
26	Update an app	Google Play	2	2
27	Send an email	Email	3	5
28	Read an email	Email	3	6
29	Make a free voice call	Viber	3	4
30	Make a free video call	Viber	3	4
31	Receive a free voice call	Viber	3	3
32	Receive a free video call	Viber	3	3
33	Receive a text message	Viber	3	4

No.	Action Name	Application	App Risk	Action Risk
34	Receive an image message	Viber	3	4
35	Receive a sound message	Viber	3	4
36	Receive a location	Viber	3	3
37	Send a free text message	Viber	3	6
38	Send a free image message	Viber	3	6
39	Send a free sound message	Viber	3	3
40	Send a location	Viber	3	5
41	Delete a message	Viber	3	6
42	Upload an image	Google Photo	3	4
43	Upload a video	Google Photo	3	4
44	Take a photo	Camera	1	1
45	Record a video	Camera	1	1
46	Save a photo	Camera	1	2
47	Save a video	Camera	1	2

Table 5-2: Actions risk

Regarding the difference between action number 8 (Receive an image message _ WhatsApp application) and 34 (Receive an image message_ Viber application), there is no difference in the final result which was a medium risk due to the medium risk could be (4 or 3). In this context, 3 means low medium risk and 4 means high medium risk. This depends on the level of impact consequences selection which was low, medium, or high.

Mobile phones can be used to capture multiple biometric modalities, such as face, voice and fingerprint recognition, by utilising microphones, cameras, keypads and GPS without disturbing legitimate mobile users. In addition, Gartner estimates that behavioural biometrics will replace passwords by 2022 (Data Protection Centre, 2018). Therefore, biometrics can be employed to substantiate whether the authenticated user is the true owner of the smartphone and thus maintain security. As a result, a wide range of biometrics were used in this research: facial,

voice, iris and fingerprint recognition, and keystroke, behavioural and linguistic profiling. EERs published in prior studies in this domain were also used in this study.

Having stated the above, if the user uses a mobile phone for reading a message/ email, watching a video, making or receiving a free call or video conference, the mobile phone might be able to capture face samples. Face ID was introduced by Apple to provide secure authentication for the iPhone X (Apple, 2018; Juniper, 2018). Apple claims that "the probability that a random person in the population could look at your iPhone X and unlock it using Face ID is approximately 1 in 1,000,000 versus 1 in 50,000 for Touch ID". In this research, a simulated scenario has been applied for generating biometric samples, a prior EER of 2% was selected for facial recognition (Tao and Veldhuis, 2010). Fingerprint profiling will also be used as transparent authentication in the near future (Feng et al., 2012; Koundinya et al., 2014). If a user uses a mobile phone at the beginning of each session, the biometric might be able to capture fingerprint samples and a prior EER was selected of 3.74% (Raghavendra et al., 2013). Furthermore, if a user uses a mobile phone to write a message or email, the biometric might be able to capture keystroke samples (Karim et al., 2018) and a prior EER of 2% was selected (Zahid et al., 2009).

For voice recognition, if a user uses a mobile phone for making/receiving a call or a video conference, the biometric might be able to capture a voice sample every 30 seconds and a prior EER of 7.80% was selected (Woo et al., 2006). Likewise, if a user uses a mobile phone for reading a message/email, watching a video, or

making or receiving a free call or video conference, the biometric might be able to capture iris samples (Du et al., 2011; Chen et al., 2012; Mock et al., 2012). Thus, a prior EER of 0.12% was chosen (Chen et al., 2012). Moreover, if a user uses more than three applications during a specific time, it might be possible to use a behavioural profiling biometric in this research and a prior EER of 7.03% was selected (Li et al., 2011). If a user uses a mobile phone for writing a message or an email, it might also be possible to capture linguistic profiling samples and a prior EER of 12.8% was selected (Saevanee et al., 2015).

In order to compute the identity confidence level, a weighted majority voting formula (Al Abdulwahid, 2017) was utilised. In this approach, for each individual biometric technique, weights are assigned that are inversely proportionate to their EERs. More specifically, the lower the EER, the higher the weight (Al Abdulwahid, 2017). Furthermore, the Python programming language was used as a processing environment (implemented on a Windows 7 Enterprise 64-bit OS with Intel Core™ i5-4310 CPU 2.7 GHz with 16 GB RAM). A number of scripts were developed in order to extract the biometric and identity confidence generated for each user to compare with the threshold, which in this research is the risk level for each action.

$$\text{Weighted Majority Voting} = \frac{\sum_{i=1}^{N}\sum_{x=1}^{M}((D_i)_x * W_i)}{\sum_{i=1}^{M} x_i}$$ (Al Abdulwahid, 2017)

Where:

- 1 is the number of the biometric technique;

- N is the total number of available biometric techniques within the specified time window;
- x is the number in the sample for the biometric technique;
- M is the total number of samples for the same biometric technique within the specified time window;
- D is the decision of the biometric sample; and
- W is the weight of the biometric technique.

NICA was selected to analyse the data and compute the identity confidence level (Clarke et al., 2009). The NICA framework was designed to be a mobile-based solution that utilises a combination of secret knowledge authentication and a number of biometric techniques, in order to provide transparent and thus continuous authentication while the user interacts with the mobile device despite the intrusive request at the beginning of the session (Clarke et al., 2009; Al Abdulwahid, 2017). In addition, the main aim of this framework is to observe the level of trust for the user in order to allow or restrict access to an application or service. Furthermore, based upon the biometric samples captured, the level of confidence fluctuates continuously (Clarke et al., 2009), which affects permissions to access applications. More specifically, if there are no biometric samples captured to cause the confidence level to exceed the threshold value, the device will be locked.

The NICA framework contains three main engines: the Authentication Engine, which is responsible for dealing with the authentication of samples and authentication decisions; the Biometric Engine, which captures and collects data

using biometric techniques; and the Authentication Manager, which is the core component of the framework and decides which authentication approach to use and manages the functionality of the framework. To provide effective security in a NICA system, different types of authentication techniques, such as biometric or secret knowledge, were allowed on the user's mobile. Furthermore, there are two security mechanisms that are considered imperative and which define the core operation of the framework: the Alert Level (AL) and the Integrity Level (IL). The two levels are mapped to confidence levels to maintain security within the system as well as usability (Clarke et al., 2009; Al Abdulwahid, 2017). During a specific time window, the AL process is used to seek valid samples. If there are no samples, the identity confidence level will be periodically reduced by the degradation function, which is 10% of current confidence in order to save power while the mobile is inactive. In the case of the mobile user requesting to perform a task, the IL is applied to check the legitimacy of that individual. If the identity confidence level is equal to or greater than the specified risk action level, transparent access is allowed. Otherwise, an intrusive authentication request is required in order to proceed with the service (see Figure 5-1). In this context, a function has been defined in NICA called a degradation function, which decreases the value of the IL (-0.5) periodically: every 30 minutes for frequent users and every 50 minutes for infrequent ones, as defined by NICA (Clarke et al, 2009), when the device is inactive.

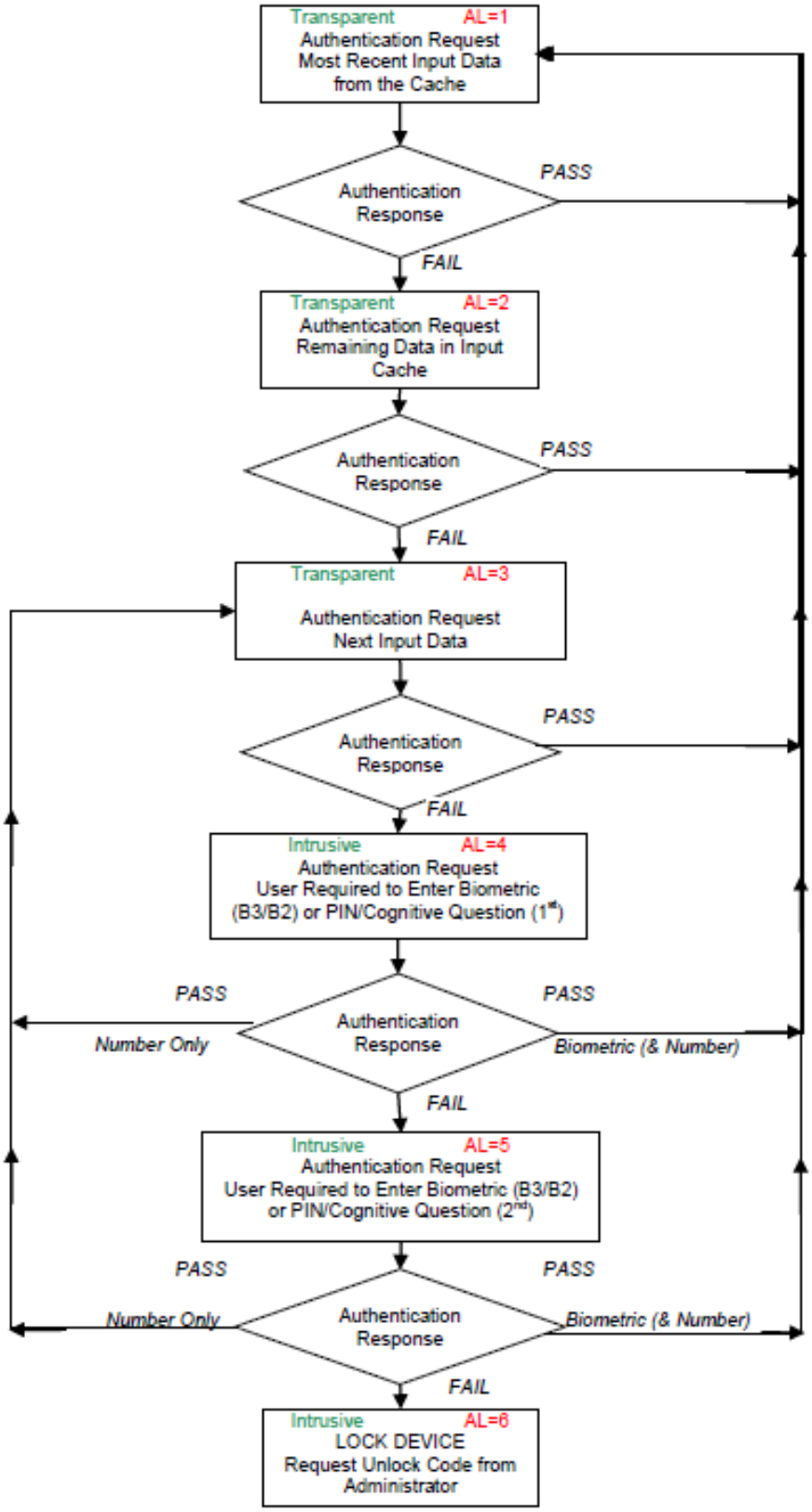


Figure 5-1: NICA Alert Level algorithm (Clarke et al., 2009)

5.2.1 Experiment Scenario 1

This experiment focuses upon the security and usability of user authentication for mobile devices using a large real-world dataset and was conducted to explore the feasibility of building a transparent and continuous biometric-based system that would provide more secure and user-friendly authentication for mobile applications. The proposed approach is based upon assessing user interactions at the intra-process (within the application) and inter-process (application access only) levels and determining whether these usage patterns will offer opportunities to link into non-intrusive, behaviour-based techniques. A Python code was written utilising ADB to collect user interactions with a mobile device. As shown in Figure 5-2, an action observation (i.e., each user file from the dataset) was produced to generate different files. The first file was produced after applying the risk model (MORI) and the second after generating possible biometric samples and then computing the identity confidence level. Finally, the two files were compared and matched at a specific time. If the confidence level is more than the threshold (action risk level), the user can access the service (non-intrusive authentication request); otherwise, the mobile device is locked (intrusive authentication request).

The above methodology was applied to each user file in order to compute the intrusive authentication requests at the intra-process (within the application) and inter-process (application access only) levels to assess the average intrusive authentication requests for all 76 users. To achieve this, a number of scripts were generated and run with the participants' data for set combinations of time windows: AL = 2 min / IL = 5 min; AL = 5 min / IL = 5 min; AL = 5 min / IL = 10 min;

AL = 10 min / IL = 10 min; AL = 20 min / IL = 10 min; and AL = 20 min / IL = 20 min. The reason for modifying the window each time was to provide further insight into whether this would affect the intrusive authentication requests for each user. After applying this methodology to 76 participants, there was a clear need to investigate how low user usage would affect the total average intrusive authentication requests. To do this, the 76 users were categorised into three usage groups (low, medium and high).

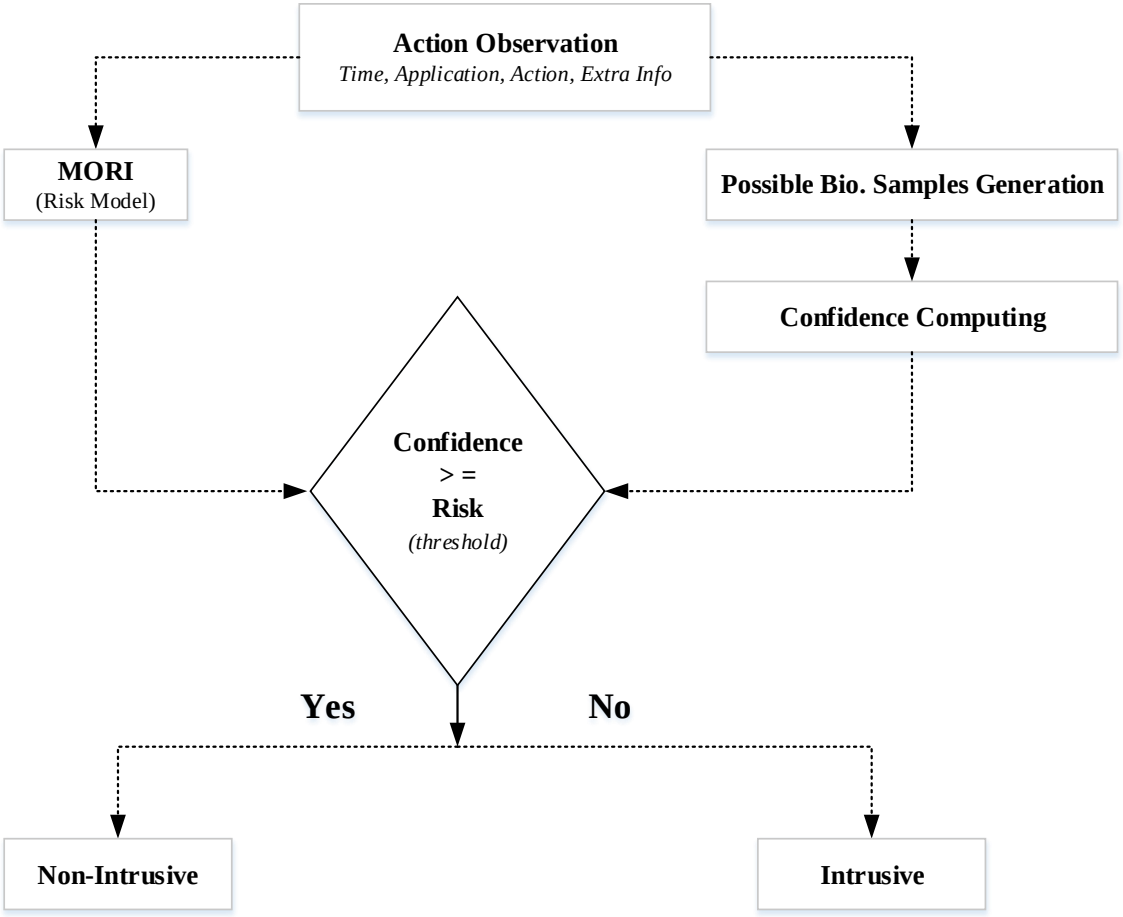


Figure 5-2: User file observation methodology

5.2.2 Experiment Scenario 2

To provide further insight into whether applying a transparent authentication system at the action level (within the application only) would enhance security and usability, the methodology for the second experiment was to compute the intra-process only for the same six time windows for the 76 participants. Digging deeper to understand how low user usage would affect the total average intrusive authentication requests was undertaken. To achieve this goal, all the participants were classified into three groups to study the differences between participants' usage, the potential impact of this on the overall performance, and to determine whether a particular grouping of time windows would perform better with a particular degree of usage.

5.2.3 Experiment Scenario 3

Further investigation was then undertaken in the third experiment to compute the inter-process (application access only) for the same six time windows for the 76 participants. The main aim of the third experiment was for evaluation purposes and to gain an insight into how useful this may be compared with the previous two experiments. All the participants were classified into three groups of usage (low, medium and high) to study the differences between participants' usage and the potential impact on overall performance. To achieve this, a code was run to calculate the average intrusive authentication requests for inter-process (application access only) only to gain greater insight into optimising performance results.

5.3 Experimental Results and Analysis

This section presents an overview of the dataset acquired, the experimental results and analysis, an investigation of the effect of different time windows on each level, and the potential for applying a transparent authentication system to intra-process security based on the dataset.

The 76 users completed the data collection process and then entered the analysis phase. Table 5-3 presents an overview of all the users' data and data collection statistics, which are arranged based on the actions per hour for each user. Each user's data were stored in an individual text file and each record contains the following fields: a date in two formats: human time and a time stamp (e.g., 2016-06-28 20:22:30, 1467141750071), application name, action type, and extra information, such as message/email length and call duration. As illustrated in Table 5-3, a large amount of user actions took place over a small number of days, as was the case with User ID (UID) 42, which suggests that this individual might be considered a very active user.

UID	Total Actions	Total Usage Days	Actions per day	Actions per hour
11	327,476	662	494	20
04	391,479	737	531	22
42	16,707	40	417	17
47	265,603	617	430	17
53	264,999	582	455	18
03	96,058	284	338	14
67	120,757	403	299	12
68	18,340	64	286	12
26	3,330	14	237	10
28	194,615	807	241	10
43	11,136	40	278	11
52	28,155	102	276	11

UID	Total Actions	Total Usage Days	Actions per day	Actions per hour
71	13,702	51	268	11
56	10,608	49	216	9
57	56,348	261	215	9
09	12,256	62	197	8
45	12,370	68	181	7
74	15,842	81	195	8
34	14,645	85	172	7
48	5,728	35	163	6
63	15,725	94	167	7
76	28,486	165	172	7
15	16,964	107	158	6
36	46,917	323	145	6
39	24,004	160	150	6
60	22,207	149	149	6
64	10,822	70	154	6
12	8,759	62	141	5
75	5,905	46	128	5
02	14,412	114	126	5
13	39,956	319	125	5
20	21,439	168	127	5
14	24,140	211	114	4
54	30,197	262	115	4
31	20,986	195	107	4
65	7,081	69	102	4
27	8,992	91	98	4
01	29,463	308	95	3
41	12,325	132	93	3
51	17,715	187	94	3
07	14,741	174	84	3
69	3,832	45	85	3
06	19,366	236	82	3
30	33,956	442	76	3
49	19,757	259	76	3
10	36,284	487	74	3
32	17,605	236	74	3
24	50,297	689	73	3
62	10,296	143	72	3
73	5,600	80	70	3
70	20,860	298	70	3
19	19,798	346	57	2
37	21,587	384	56	2
22	18,457	337	54	2

UID	Total Actions	Total Usage Days	Actions per day	Actions per hour
44	34,202	637	53	2
55	22,933	424	54	2
33	29,018	549	52	2
29	14,254	285	50	2
05	61,205	1230	49	2
21	21,880	443	49	2
50	21,269	431	49	2
66	47,319	984	48	2
46	27,576	592	46	1
38	14,807	333	44	1
72	15,068	346	43	1
08	14,986	343	43	1
61	14,496	361	40	1
23	6,970	175	39	1
40	10,314	261	39	1
59	4,967	138	35	1
25	4,226	131	32	1
16	20,378	644	31	1
35	8,394	271	30	1
18	8,390	280	29	1
58	10,079	349	28	1
17	23,523	818	28	1

Table 5-3: Data collection statistics

The overall final captured dataset statistics from the 76 participants are summarised and presented in Table 5-4. This amount of information was felt to be sufficiently rich to allow meaningful analysis; that is, 22,457 days of mobile usage.

Total Number of All Users	76
Total Number of Days	22,457
Average Number of Days per User	136
Total Number of Voice Calls	101,882

Length of Voice Calls	36,566 hours
Total Number of SMS Messages	2,598,164 SMS messages
Length of SMS Messages	124,117,633 characters
Total Number of Email Messages	14,289 email messages
Length of Email Messages	2,813,960 characters
Total Number of Actions Accessed	3,006,092

Table 5-4: Overall final captured dataset statistics

Table 5-5 shows how many sample points there were for each application. It is clear from the table that WhatsApp was the most frequently accessed application, whereas the other applications taken together were accessed a total of 252,770 times. In this context, the five most commonly used applications among the participants were WhatsApp, Google Play, SMS, Email, and Browser. Although the Viber app was ranked second to WhatsApp in the application samples, with 118,426, as shown in Table 5-5, it was not commonly accessed among the participants as a whole.

Application Name	**Total Number of Times Accessed**
WhatsApp	2,753,322
Viber	118,426

Google Photo	49,578
Camera	25,261
Email	14,289
Phone Call	13,808
Browser	10,785
SMS	8,459
Downloading	8,341
Google Play	3,251
YouTube	572

Table 5-5: Total number of applications accessed

Table 5-6 demonstrates the total number of actions for each user for the selected applications in this dataset. It is clear from the table that the top three ranked user actions were for WhatsApp. This in turn means that WhatsApp gained the highest amount of usage among all the participants.

Action Name	**Total**	**Action Name**	**Total**
Receive a text message_ WhatsApp	1,662,768	Send a text message_ WhatsApp	824,207
Receive image message_ WhatsApp	117,413	Make a free video Call_Viber	58,784
Send free sound message_ Viber	49,578	Receive a video message_WhatsApp	45,191
Receive image message_ Viber	43,946	Send an image message_WhatsApp	40,939
Receive audio message_ WhatsApp	25,753	Send a location_Viber	23,308
Take a photo_ Camera	23,308	Send an email_Email	13,965
Receive a free call (voice/video)	12,451	Search_Browser	10,643
Make free call(voice/video)_WhatsApp	9,751	Download a file_Downloading	8,341
Make a call_ Phone Call	7,606	Receive a sound message_Viber	6,28
Receive a call_ Phone Call	6,202	Send a video message_WhatsApp	6,029

Send an audio message_WhatsApp	5,970	Receive a free voice call_ Viber	5,144
Read a SMS message_ SMS	5,101	Send an SMS message_ SMS	3,358
Download app_Google Play	3,251	Receive a location_ Viber	2,779
Upload image_ Google Photo	1,130	Save a photo_ Camera	1,130
Receive a free video call_ Viber	1,066	Receive a PDF file_ WhatsApp	1,016
Receive a contact card_ WhatsApp	842	Delete a message_ Viber	822
Record a video_ Camera	822	Search on YouTube_ YouTube	572
Receive a location _ WhatsApp	517	Read an email_ Email	325
Update app_ Google Play	324	Send a contact card_ WhatsApp	192
Send a PDF file_ WhatsApp	162	Watch a video_ Browser	142
Make a free voice call_ Viber	139	Send a location_ WhatsApp	121
Send free image message_ Viber	10	Send a free text message_ Viber	4
Receive a text message_ Viber	1	Upload video_ Google Photo	1
Save a video_ Camera	1		

Table 5-6: User action statistics

Examining the distributions of user hours for all the participants in greater depth, as shown in Appendix D, the histogram in Figure 5-3 highlights the differences that might be considered significant compared with the total population. For instance, the user profile for participant 71 can be differentiated from the others due to the mobile phone mainly being used from 00:00 AM until 6:00 AM, whereas the majority of participants used their mobile phones from 8:00 AM to 10:00 PM. On the other hand, four participants (42, 47, 53, and 68) show identical usage compared with the population.

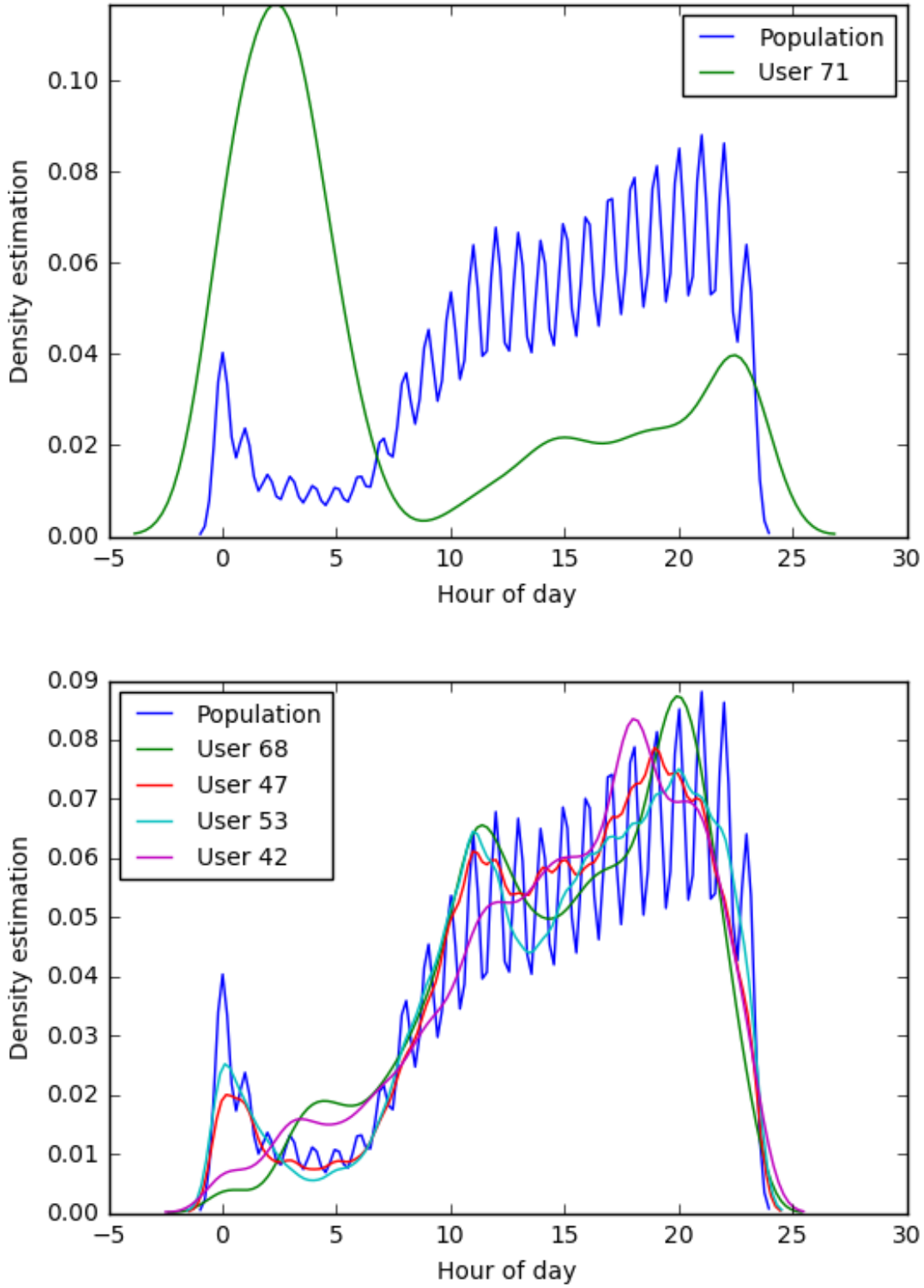


Figure 5.3: Histogram for population compared with partipents

Figure 5-4 demonstrates the dataset for the sample after applying the risk model to the original dataset for a very short period. As shown in the figure, user activity and interaction are shown with the risk levels for the different types of applications. For instance, the WhatsApp application has different processes, which has an impact on the data and involves different levels of risk. There is no single risk involved when using the WhatsApp application. For instance, sending a message on WhatsApp does not have the same risk when compared with receiving a free call on the same application. This suggests that different levels of security controls should be applied to data based on the risk level in order to deny unauthorised access to the content of the application. This system would, in turn, facilitate control of the overall authentication process, thereby enabling a continuous and non-intrusive authentication approach. This method could also be applied continuously and transparently without impeding the user's actions.

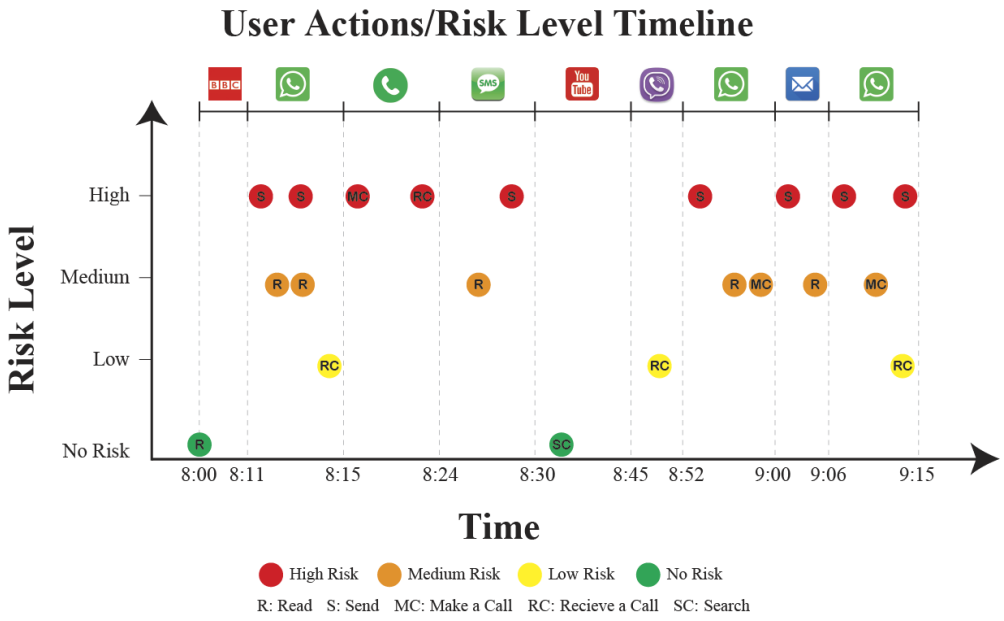


Figure 5-4: User actions with risk level timeline

It would be useful to better assess the performance of this research under different scenarios, to improve the acquired results and determine whether a particular grouping of time windows would perform more effectively with a particular type of usage. For this purpose, the participants were divided based on the average number of actions per hour, as shown in Table 5-3. The diversity of users' interactions is clear from this table. Based on this dataset, average actions per hour was calculated and find 5 actions and more consider high usage. For instance, participant 4 seems to have been a very active user due to undertaking 22 actions per hour during 737 days of 391,479 actions, while participant 25 achieved only one action per hour during 131 days of 4,226 actions. Based on the information shown in Table 5-3, the users were classified into three groups: low usage, medium usage, and high usage, as follows:

- If (Actions per hour) > 5, then High Usage
- Elseif (Actions per hour) > 2, then Medium Usage
- Elseif Low Usage

Table 5-7 shows the usage type for all the participants.

Usage Type	User ID
High Usage	3,4,9,11,15,26,28,34,36,39,42,43,45,47,48,52,53,56,57,60,63,64,67,68,71,74,76
Medium Usage	1,2,6,7,10,12,13,14,20,24,27,30,31,32,41,49,51,54,62,65,69,70,73,75
Low Usage	5,8,16,17,18,19,21,22,23,25,29,33,35,37,38,40,44,46,50,55,58,59,61,66,72

Table 5-7: Usage type for each user

Figures 5-6 and 5-7 demonstrate examples of action requests for user 47 (high usage user) and user 72 (low usage user) throughout one day, respectively, associated with the action risk after applying the risk model. As illustrated in Figure 5-6, it appears that there is no single risk to using a given application, since the risk changes within the application from one process to another. Therefore, there is a clear need to define a suitable level of security by enabling intra-process security, as this would permit a far more robust approach to confirming the authenticity of the user. The two figures indicate that it would be useful to move an access control system from being on an application to within the application based on the risk level for each process and to establish appropriate levels of security. Another observation relating to the same figures is that the vast majority of the actions were considered to have a high or medium risk, which, in turn,

suggests it is important to apply appropriate protection to data by understanding the nature of the risk involved.

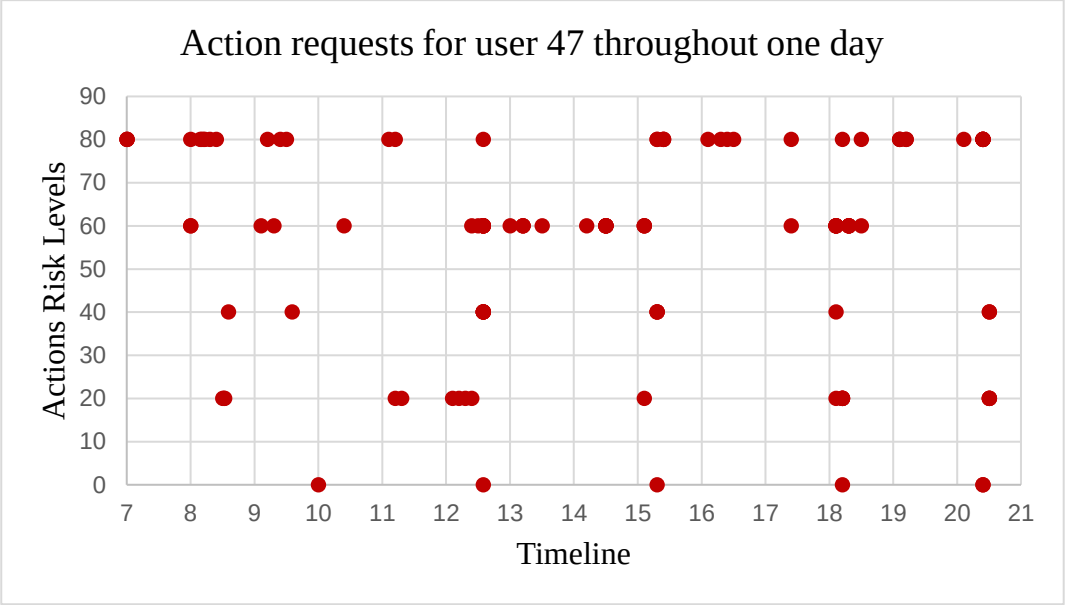


Figure 5-6: Action requests for user 47 throughout one day (high usage user)

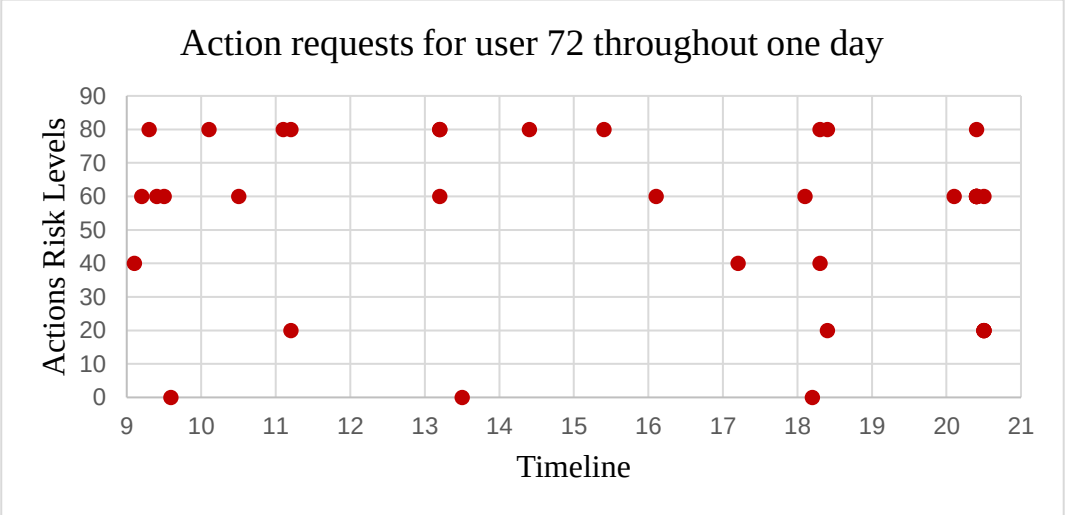


Figure 5-7: Action requests for user 72 throughout one day (low usage user)

5.3.1 Experiment 1: Biometric TAS for Intra- and Inter-process Access

The main aim of this experiment was to test the inter- and intra-process impact on the overall transparent user authentication approach to mobile applications by comparing access with other actions within the application for the 76 participants. To do this, the average intrusive authentication requests were computed and demonstrated for both the intra-process (within the application) and inter-process (application access only) levels in this experiment. Based on the methodology, as shown in Figure 5-2, the 76 users were then classified into three groups of usage (low, medium and high). The code was run with the participants' data. The experimental results and analysis were shown and used to investigate the effect of classifying the 76 participants into three groups of usage on the different time windows for each level and the potential for applying the transparent authentication system to intra- and inter-process security. Figure 5.8 shows the confidence level with intrusive authentication time line for the user after matching two files: the actions file and the confidence file at a specific point in time.

The following figures provide examples of the relation between identity confidence and intrusive authentication requests on a timeline for high user usage, low user usage and medium user usage. In Figure 5.8, the user confidence level fluctuates continuously based on the biometric samples captured, as does the risk level for the user action. Although there is high fluctuation over this period, only one intrusive authentication request was triggered due to the biometric samples captured, thereby raising the identity confidence level for participant 57. In contrast, three intrusive authentication requests were made in relation to the

low usage of user 8. As shown in Figure 5.9, the participant did not use his/her mobile between 12:21 PM and 14:16 PM and no biometric sample could be captured. For this reason, the confidence level was equal to zero and, therefore, the user was asked to enter a password or fingerprint for the authentication process. Similarly, no biometric samples could be captured between 11:46 AM and 12:17 PM for participant 7, as shown in Figure 5-10 and, as a result, the identity verification level decreased. However, the user's confidence was very high after 14:16 PM, which suggests that the mobile user might be able to make a high-risk action. As a consequence, the more time between two consecutive actions, the higher the intrusive authentication requests.

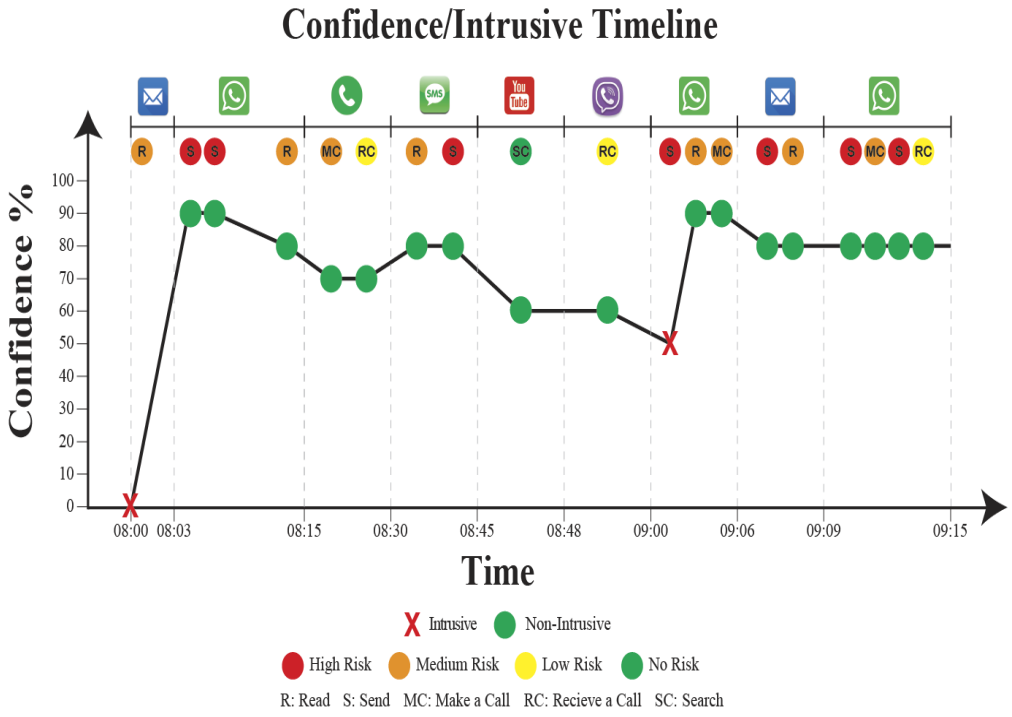


Figure 5-8: Confidence with intrusive timeline for participant 57 (high user usage)

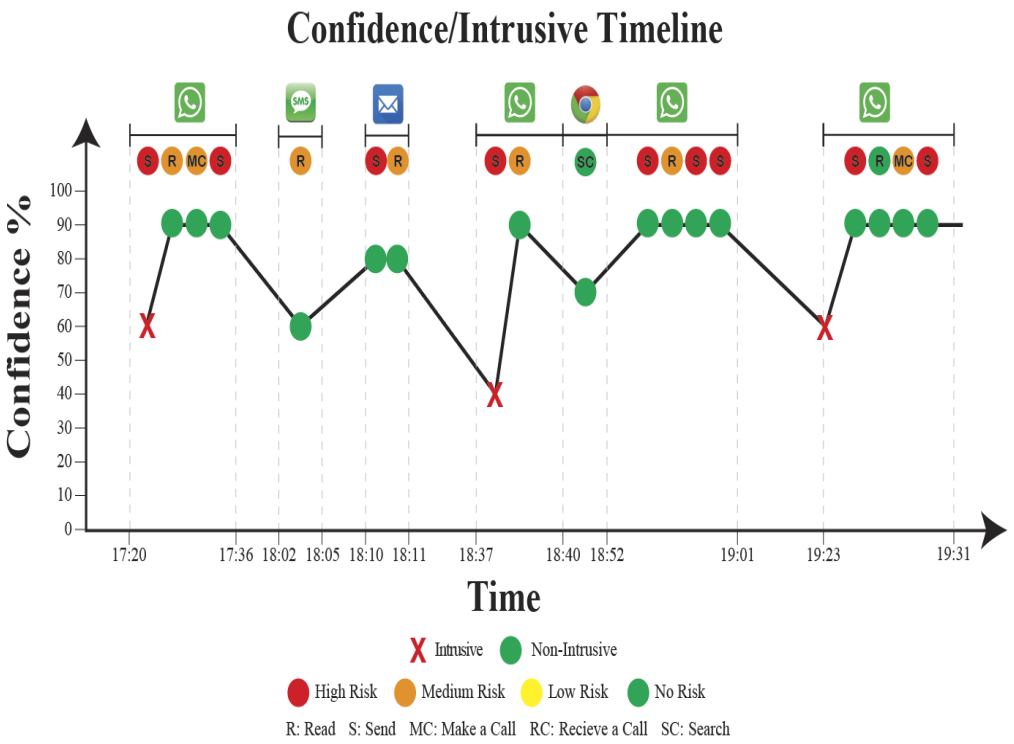


Figure 5-9: Confidence with intrusive timeline for participant 8 (low user usage)

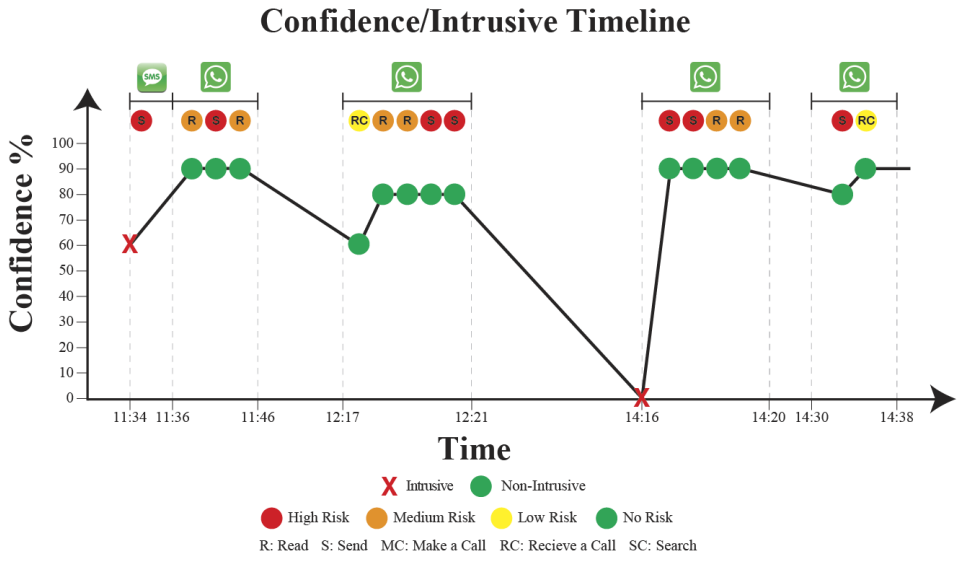


Figure 5-10: Confidence with intrusive timeline for participant 7 (medium user usage)

Figure 5-11 shows the average user intrusive requests distribution for intra-process (within the application) and inter-process (application access only) based on the minimum, median and maximum values over the various time windows. As depicted in Figure 5-11, the largest time window (AL = 20 min / IL = 20 min) achieved better results due to the majority of the average users' intrusive requests distribution being less than 10% of the total average users' intrusive requests. For instance, participant 35 achieved 13% intrusive authentication requests. In contrast, the shortest time window (AL = 2 min / IL = 5 min) achieved the worst result due to the majority of the average users' intrusive requests distribution among the total requests being about 20%. For instance, the average intrusive requests for three participants (2, 29, and 46) were 37%, 36% and 38%, respectively. Interestingly, when the AL was the same value (i.e., AL = 10 min / IL = 10 min and AL = 10 min / IL = 20 min), the average users' intrusive requests distribution was still the same and the majority were less than 9%. Similarly, the AL = 5 min / IL = 5 min and AL = 5 min / IL = 10 min time windows were the same but the majority were close to 15%.

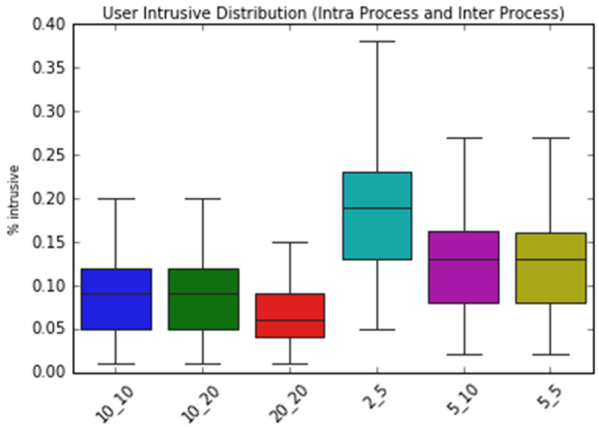


Figure 5-11: Average user intrusive requests distribution

To summarise, the experimental results for the percentages of intrusive authentication requests for the six time windows for intra-process (within the application) and inter-process (application access only) were calculated and are shown in Table 5-8, together with the numbers of intrusive users. In this table, it is clear that the average intrusive requests decreased, ranging from 18% to 6%. In general, the larger the AL/IL, the fewer the number of intrusive authentication requests. This could be because there is a high probability of capturing many of the biometric samples required when users interact with their mobile device for long intervals and the degradation function is not recalled to reduce the identity confidence when the device is inactive. However, this was not the case for short intervals and suggests that this does not allow the mobile user to increase his/her identity confidence level if there is a low number of actions. In this context, the longest time window (AL= 20 min / IL= 20 min) attained the lowest percentage of average intrusive requests (6%), which might favour usability but not security. This could be due to there not being any samples taken while the degradation function is inactive during a short interval. More specifically, for the time window AL = 2 min / IL = 5 min, six participants (2, 12, 29, 46, 55, 58) achieved more than 30% of the intrusive requests due to the total number of actions being very small compared with the total usage days and the actions per day. For instance, 27,576 actions were collected from user 46 over 592 days, which represents about 46 actions per day. This low number of actions during the course of a day led to the highest percentage of intrusive requests for all the users (38%) and might affect the total average authentication requests (18%), as shown in Table 5-8.

		Time Window					
		AI = 2	AI = 5	AI = 5	AI = 10	AI = 10	AI = 20
		IL = 5	IL= 5	IL= 10	IL= 10	IL= 20	IL= 20
Intra + Inter	% Average Intrusive Requests	18	13	13	9	9	6
	Total Requests	3,006 k					
	Intrusive ≤ 10% (# users)	16	29	27	45	46	67
	10% < Intrusive ≤ 15%	10	24	28	24	23	9
	15% < Intrusive ≤ 20%	21	9	14	6	6	0
	Intrusive > 20%	29	14	7	1	1	0

Table 5-8: Average percentages of intrusive authentication requests

One possible reason is that, in the data collection stage, 47 actions were collected with the following distribution of risk types: 36% were high risk, 47% were medium risk, 13% were low risk, and 4% were no risk. As a result, the majority of these actions were considered high and medium risk (83%). Figures 5-12 and 5-13 show the intrusive/non-intrusive request results for the types of risk for all time windows.

In Figure 5-12, it is apparent that the majority of intrusive requests were the result of a high-risk action, a few from a medium-risk action and none from low-risk

actions. For instance, in the AL = 2 min / IL = 5 min time window, 16% of the total average intrusive requests (18%) were triggered by high-risk actions and only 2% of the total average intrusive requests came from medium-risk actions.

Similarly, it is clear from Figure 5-13 that the majority of intrusive/non-intrusive request results came from low-risk actions (AL = 10 min / IL = 10 min, AL = 20 min / IL = 20 min and AL = 10 min / IL = 20 min); only 1% came from medium-risk actions and 8% from high-risk actions in comparison with the total average intrusive requests for the other time windows (AL = 2 min / IL = 5 min, AL = 5 min / IL = 5 min, and AL = 5 min / IL = 10 min).

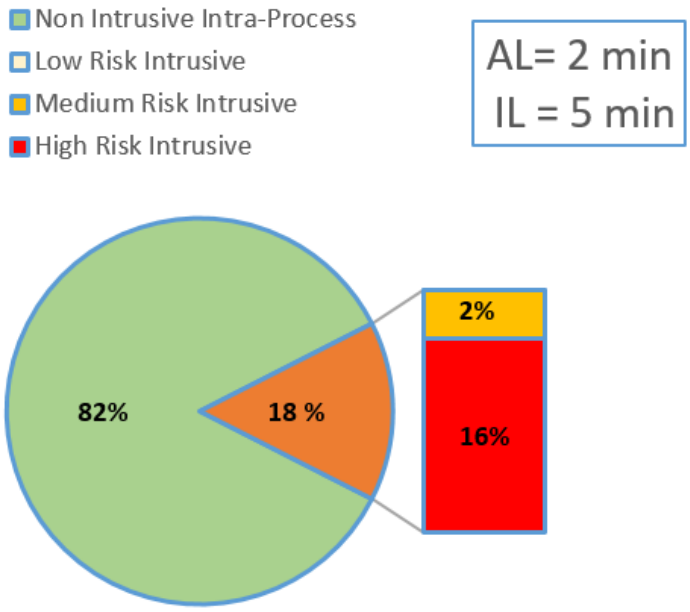


Figure 5-12: Intrusive/non-intrusive requests for intra/inter-process, AL= 2 min / IL= 5 m

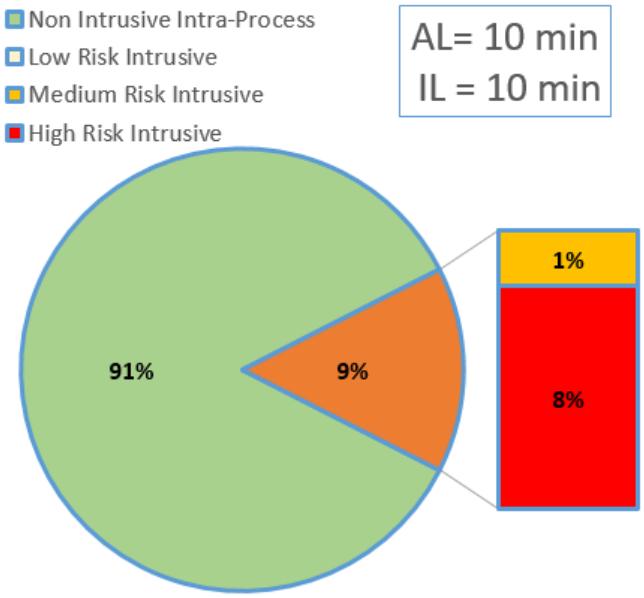


Figure 5-13: Intrusive/non-intrusive request results for intra-/inter-process at AL= 10 min / IL = 10 min

To gain greater insight into how low usage might affect the total average intrusive authentication requests for the entire dataset, the participants were categorised into three levels of group usage and the total average intrusive authentication requests were re-computed for each group. To do this, the time window AL = 10 min / IL = 10 min was selected in order to demonstrate the effect of changing the time window on each group of usage, as shown in Figure 5-14. It is clear that the time window AL = 10 min / IL = 10 min achieved better results among the high usage group as 95% of users' intrusive authentication requests being under 8%. Similarly, for the medium usage group, 77% of users' intrusive authentication requests were under 12%, although half the users' intrusive authentication requests were more than 14% for the low usage group. As a result, these experimental results suggest that a time window of AL = 10 min / IL = 10 min could be used effectively with high and medium usage groups.

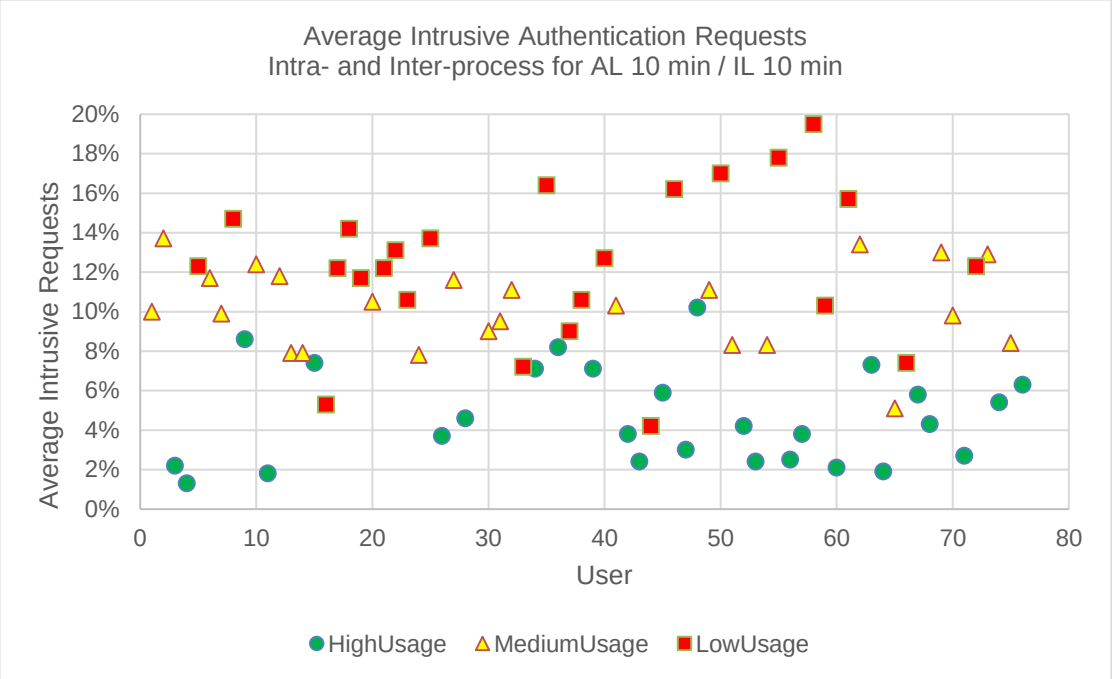


Figure 5-14: Average intrusive authentication requests at the intra- and inter-process levels (AL = 10 min / IL = 10 min)

Based on the above analysis of the experimental results for the percentage of intra- and inter-process intrusive authentication requests, the total requests for the six time windows were calculated and are summarised in Table 5-9. In this table, it is clear that this approach achieved the best results following the classification of the participants into three groups of usage to identify the most suitable time window for each group. The table also shows that the larger the AL/IL, the fewer the number of intrusive authentication requests due to the high probability of being able to gather biometric samples when users interact with their mobile device and the degradation function is not recalled to reduce the identity confidence when the device is inactive. In Table 5-9, the percentages of intrusive authentication requests achieved were improved when compared with those previously reported in the first experiment for all the AL/IL timings. For

instance, for the same time window (AL = 5 min / IL = 5 min), the percentage of average intrusive authentication requests for all users was 13% but this was reduced to 7% for the high usage group. On the other hand, the percentage of average intrusive increased to 21% after grouping the users.

Furthermore, the number of participants whose percentage of intrusive authentication requests was less than 10% sharply increased and represent the majority of participants for all the AL/IL timings. Interestingly, only one participant (58) achieved a percentage of intrusive authentication requests of about 16% for the AL = 20 min / IL = 20 min time window. As can be seen in Table 5-9, the change in the average intrusive authentication requests between time windows was clear at the action level when compared with the application level.

		Time Window Intra + Inter					
		AI = 2	AI = 5	AI = 5	AI = 10	AI = 10	AI = 20
		IL = 5	IL= 5	IL= 10	IL= 10	IL= 20	IL= 20
High Usage	% Average Intrusive Requests	12	7	7	5	5	3
	Total Requests	2,045 k					
	Intrusive ≤ 10% (# users)	6	21	21	27	27	27
	10% < Intrusive ≤ 15%	14	6	6	0	0	0
	15% < Intrusive ≤ 20%	5	0	0	0	0	0
	Intrusive > 20%	2	0	0	0	0	0
Medium Usage	% Average Intrusive Requests	21	15	15	10	10	7
	Total Requests	464,869					
	Intrusive ≤ 10% (# users)	1	2	2	13	13	24
	10% < Intrusive ≤ 15%	2	14	14	11	11	0
	15% < Intrusive ≤ 20%	10	7	7	0	0	0
	Intrusive > 20%	11	1	1	0	0	0
Low Usage	% Average Intrusive Requests	22	16	16	13	13	9
	Total Requests	496,096					
	Intrusive ≤ 10% (# users)	1	4	4	6	6	16
	10% < Intrusive ≤ 15%	3	7	7	12	12	9
	15% < Intrusive ≤ 20%	7	8	8	7	7	0
	Intrusive > 20%	14	6	6	0	0	0

Table 5-9: Average percentages of intrusive authentication requests for usage

It appears that the largest time window achieved a good result and reduced the number of intrusive authentication requests. For instance, the average intrusive authentication requests for AL = 10 min / IL = 10 min were fewer than the AL = 5 min / IL = 5 min time window by 2% at the action level, while there was no change at the application level of 4%. The change was clear for participants 28 and 48 by 5% and 2%, respectively. Interestingly, the experiment results for participant 71 for both time windows was the same for intrusive authentication requests at 3%. Furthermore, intrusive authentication requests changed very slightly (by 1%) for

some participants, such as 3, 4, 11, 53, 60 and 64. On the other hand, there was a large difference at the action level between two time windows (AL = 5 min / IL = 5 min and AL = 10 min / IL = 10 min) for participants 15, 48, and 67, as the intrusive authentication requests were reduced by 5% at the action level.

It also seems that, for the medium usage group, the longer time windows achieved equally good results and the intrusive authentication requests were reduced. Participants 2 and 12 achieved better results regarding intrusive authentication requests at the action level (ranging from 14% to 7% and from 12% to 6%, respectively). Similarly, for the low usage group, the longer time windows achieved better results (ranging from 9% to 7% at the action level). Interestingly, the intrusive authentication requests changed very slightly (by 1%) for some participants, such as 5, 22, and 72. There was a significant difference at the action level for participants 29 and 46, as their intrusive authentication requests reduced by 3% (participant 29 ranging from 14% to 11%). It appears that the majority of users achieved intrusive requests of less than 10%.

5.3.2 Experiment 2: Biometric TAS for Intra-process Access

To provide further insight into whether applying a transparent authentication system at the action level would enhance security and usability, this experiment was applied to each user file to compute the average intrusive authentication requests for all 76 users. This second experiment differs from the first by focusing on user action access only (intra-process access) and not application access (inter-process access). To do this, after applying the risk model, the code was run with the participants' data to generate biometric samples (based on AI

Abdulwahid, 2017) and then calculate the confidence level and intrusive authentication requests for each user for each user action by utilising NICA across various ALs and ILs with the actions (within application only). The reason for trying different combinations of time windows was to investigate their effect on the system performance. As demonstrated in Figure 5-15, the distribution of user intrusive requests for 76 participants on an intra-process level based on minimum, median, and maximum values over the different time windows was considered. In this figure, and as mentioned in Table 5-10, the majority of user intrusive requests for the AL = 2 min / IL = 5 min time window were between 15% and 20% for 26 users. For instance, participant 46 had the highest intrusive requests at 33%, whereas participant 71 had 4% intrusive requests. It can be interpreted from these results that the total usage of these participants played a significant role. In this context, the total usage for participant 46 was 27,576 over 592 days, which, in turn, means one action per hour approximately. This low usage could have led to the poor performance and is likely to lead to a large number of intrusive requests.

On the other hand, the highest usage might be the cause of the fewest intrusive requests, such as participant 71 with a usage of 13,702 over 51 days, which, in turn, means three actions per hour approximately. In contrast, the vast majority of user intrusive requests for the AL = 20 min / IL = 20 min time window were less than 10% (73 participants) which was envisaged to be the case given the longer length of time to collect biometric samples or a longer time in which to recall the degradation function to reduce the user identity level. Another observation

regarding this figure is that the result was mostly identical if there was no change in the AL value, such as AL = 5 min / IL = 5 min and AL = 5 min / IL = 10 min, which could suggest that AL is important.

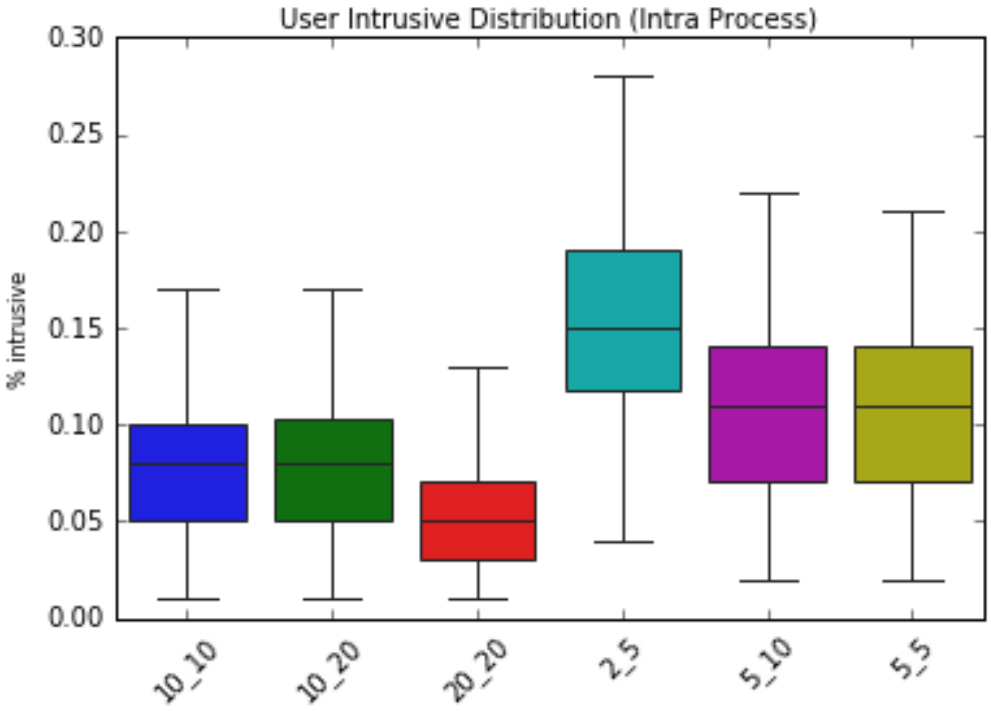


Figure 5-15: Average user intrusive requests distribution for intra-process access

As depicted in Table 5-10, the performance results for experiment 2 across various ALs and ILs were promising for the intra-process level (actions within application only). The experimental results range from 15% average intrusive authentication requests at AL = 2 min / IL = 5 min to 5% at AL = 20 min / IL = 20 min for the same total of requests (2,561k). Accordingly, it is clear from Table 5-10 that the more substantial the AL and IL values, the fewer intrusive authentication requests. This is logical, as in cases in which the biometric samples were insufficient or not available for capture, the user identity was

reduced by the degradation function and resulted in a high FRR for the smaller time windows. For instance, the percentage of average intrusive authentication requests gradually reduced by approximately 50% for the AL = 10 min / IL = 10 min window to 7% from 15% for AL = 2 min / IL = 5 min. As a result, the shorter time windows could have the effect of raising the security level in relation to users' convenience, which was the opposite case for the larger time windows. The larger time windows might also lead to preserving a high level of identity confidence even though no biometric samples could be captured, which means there is an opportunity for misuse of the mobile device by an unauthorised user.

		Time Window					
		AL = 2	AL = 5	AL = 5	AL = 10	AL = 10	AL = 20
		IL = 5	IL = 5	IL = 10	IL = 10	IL = 20	IL = 20
Intra	% Average Intrusive Requests	15	10	11	7	8	5
	Total Requests	2,561 k					
	Intrusive ≤ 10% (# users)	20	37	37	58	57	73
	10% < Intrusive ≤ 15%	18	34	29	17	17	2
	15% < Intrusive ≤ 20%	26	4	6	1	2	1
	Intrusive > 20%	12	1	4	0	0	0

Table 5-10: Percentages of intrusive authentication requests for intra-process access

As previously mentioned, in the data collection stage, 47 actions were collected with the following distribution of risk types: 36% were high risk, 47% were medium risk, 13% were low risk, and 4% were no risk. One possible reason for the high percentage of intrusive authentication requests for some participants is that the majority of these actions are considered high and medium risk (83%), so the threshold (i.e., risk level) would require a greater confidence value to access the service.

In this context, Figures 5-16 and 5-17 show the intrusive/non-intrusive request results for the types of risk for the AL = 2 min / IL = 5 min and AL = 10 min / IL = 10 min time windows, respectively, for intra-process access. In both figures, the majority of intrusive requests come from high-risk actions, leading to an increase in the average intrusive authentication requests. Only 3% of the total requests come from medium-risk actions for the AL = 2 min / IL = 5 min time window.

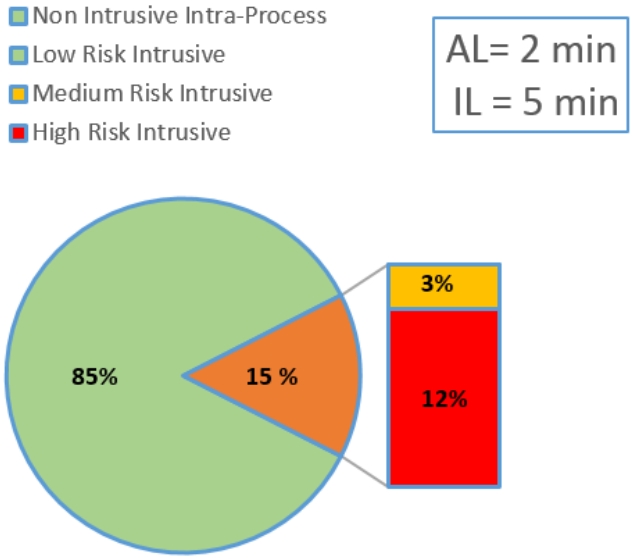


Figure 5-16: Intrusive/mon-intrusive request results for intra-process access at AL = 2 min / IL = 5 min

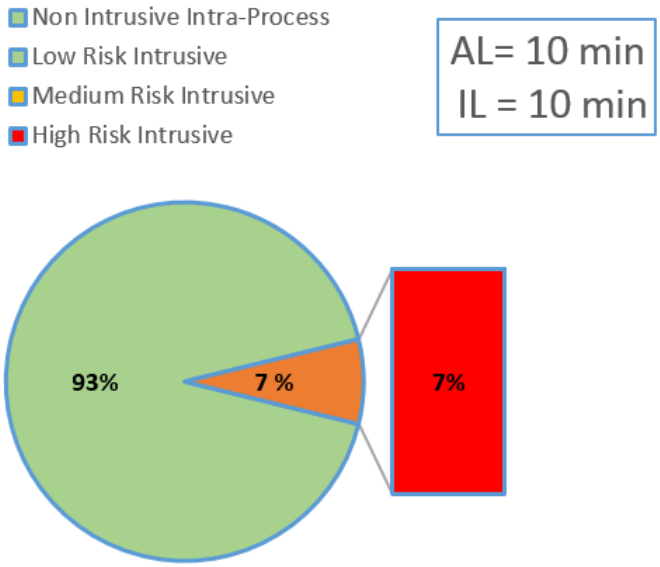


Figure 5-17: Intrusive/non-intrusive results for intra-process access at AL = 10 min / IL = 10 min

The experimental results clearly demonstrate that the proposed framework is able to provide a transparent authentication system for intra-process security. In addition, paying closer attention to the intrusive request results for different types of usage might lead to reducing the total average intrusive requests. For instance, participants 46, 71 and 57 received intrusive requests of 33%, 4% and 6%, respectively, for the shortest time window (AL = 2 min / IL = 5 min). To assess this, the 76 participants were categorised into three usage groups based on the user actions per hour, as previously mentioned in Table 5-4. The primary aim of the participant categories was to gain greater insight into how low usage would affect the total average intrusive authentication requests for the entire dataset. The categorisation was also aimed at testing whether all the time windows

considered were reasonable and would tend to be more suitable for different types of users and thereby affect the intrusive authentication requests.

As previously mentioned in Table 5-7, the experimental results for the 76 participants were categorised into three groups of usage (27 users had high usage, 24 users had medium usage, and 25 users had low usage), as shown in Table 5-8. Accordingly, it can be seen that the results significantly improved following this classification and could lead to gradually reduced intrusive authentication requests. For instance, participants 36, 67, and 15 attained the highest average intrusive authentication requests at 18%, 17%, and 15%, respectively, for the shortest time window (AL = 2 min / IL = 5 min), whereas they achieved 4%, 2%, and 3%, respectively, with the largest time window (AL = 20 min / IL = 20 min). A possible reason for this is that there is sufficient time to find and capture biometric samples, thereby raising the user identity level with enough time to reduce the confidence level (IL = 20 min).

For the same group of usage, however, participants 71, 4, and 60 obtained the lowest average intrusive authentication requests of 4%, 5%, and 5%, respectively, with the shortest time window (AL = 2 min / IL = 5 min). Similarly, they achieved 3%, 2%, and 3%, respectively, with the largest time window (AL = 20 min / IL = 20 min), which was expected to have fewer intrusive authentication requests. What can also be noticed in Table 5-11 is that the vast majority of participants achieved less than 10% intrusive authentication requests across all the different time windows (ranging from 15 participants at AL = 2 min / IL = 5 min to 27 participants at AL = 10 min / IL = 10 min).

		Time Window **Intra-process**					
		AL = 2	AL = 5	AL = 5	ALn = 10	AL = 10	AL = 20
		IL = 5	IL = 5	IL= 10	IL = 10	IL = 20	IL = 20
High Usage	% Average Intrusive Requests	10	6	6	4	4	2
	Total Requests	1,772 k					
	Intrusive ≤ 10% (# users)	15	26	26	27	27	27
	10% < Intrusive ≤ 15%	9	1	1	0	0	0
	15% < Intrusive ≤ 20%	3	0	0	0	0	0
	Intrusive > 20%	0	0	0	0	0	0
Medium Usage	% Average Intrusive Requests	18	12	13	9	9	6
	Total Requests	396,640					
	Intrusive ≤ 10% (# users)	1	5	5	19	19	24
	10% < Intrusive ≤ 15%	4	17	14	5	5	0
	15% < Intrusive ≤ 20%	12	2	4	0	0	0
	Intrusive > 20%	7	0	1	0	0	0
Low Usage	% Average Intrusive Requests	18	13	13	10	10	8
	Total Requests	392,795					
	Intrusive ≤ 10% (# users)	4	7	7	13	13	23
	10% < Intrusive ≤ 15%	6	15	15	11	11	2
	15% < Intrusive ≤ 20%	9	2	2	1	1	0
	Intrusive > 20%	6	1	1	0	0	0

Table 5-11: Average percentages of intrusive authentication requests for intra-process (usage)

On the other hand, for the medium and low usage groups, a further interesting point to be noticed in these results is that the average intrusive authentication requests increased compared with the entire dataset for the same time windows (15% vs 18%). In addition, the vast majority of participants achieved around 15% intrusive authentication requests across the shorter time windows. For instance, at medium usage, participant 21 has the highest percentage of intrusive requests (25%) due to 21,880 actions being produced over 443 days, which means two

actions per hour. In contrast, participant 65 has the lowest intrusive requests of 6%. These results support the conclusion that a short time window might mean the required service is protected by intrusive requests if no interaction is performed between the mobile user and his/her device and biometric samples are not available. Although the short time windows prompted a high degree of protection and intrusive authentication, this intrusiveness might lead to exaggerated re-authentication of the original user. As a result, short time windows appear to work well for security but are not quite sufficient for usability.

With regard to the low usage group results, approximately 56% of user intrusive requests were more than 15% for the shortest time window. For instance, participants 46 and 58 achieved 33% and 28%, respectively, which are the highest percentages of intrusive requests, whereas participant 44 achieved a much lower rate of intrusive requests (6%). In addition, the intrusive requests for this participant improved to 2% for the longest time window (AL = 20 min / IL = 20 min). One of the reasons for this could be that the degradation function was recalled very few times due to the AL taking a long time to collect biometric samples, thereby increasing the probability of raising the user identity level. Therefore, a larger time window can be considered to perform well with the majority of low user usage.

5.3.3 Experiment 3: Biometric TAS for Inter-process Access

The main aim of the third experiment was evaluation and to gain insight into how useful this approach may be. The methodology for this experiment was to compute the inter-process (application only) access for the same six time

windows for the 76 participants. All the participants were then classified into three groups of usage (low, medium and high) to study the differences between the participants' usage and the potential impact on overall performance. To do this, the code was run to calculate only the average intrusive authentication requests for inter-process (application only) access.

		Time Window					
		AL= 2	AL = 5	AL = 5	AL = 10	AL = 10	AL = 20
		IL = 5	IL= 5	IL= 10	IL= 10	IL= 20	IL= 20
Inter	% Average Intrusive Requests	56	48	48	40	40	31
	Total Requests	104,245					
	Intrusive ≤ 10% (# users)	4	5	5	4	4	8
	10% < Intrusive ≤ 15%	0	0	0	3	3	7
	15% < Intrusive ≤ 20%	0	1	1	5	7	2
	Intrusive > 20%	72	70	70	64	62	59

Table 5-12: Average percentages of intrusive authentication requests for inter-process

Table 5-12 presents the performance results for experiment 3 across various ALs and ILs for the inter-process level (actions within application only). As seen in the table, the experimental results for all the time windows achieved a high percentage of intrusive authentication requests, ranging from 56% to 31%. In addition, there were a total of 104,245 application requests, which was very low compared with the intra-process and inter-/intra-process results of 2,561k and 3,006k, respectively. The results of classifying all the participants into three groups of usage (low, medium and high) still achieved a high percentage of intrusive authentication requests. More specifically, these range from 44% to 19% for the high usage group, from 66% to 38% for the medium usage group, and from 59% to 39% for the low usage group. In general, the inter-process results indicated that this did not perform very well in comparison with the two previous experiments (i.e., experiment 1: intra- and inter-process; experiment 2: intra-process). The high percentage of intrusive authentication requests could be due to the low level of confidence as the confidence decreased according to the AL interval if no biometric samples could be captured. In this case, there is a clear need to force the user to raise his/her biometric confidence level, either by the use of a password or by providing valid biometric modalities.

To address this problem, the median is suggested, thereby offsetting the shortcoming. The difference in time between two consecutive app access requests is calculated and, if the resulting value is greater than the median, a new app request is generated. Table 5-13 shows the lower intrusive rate achieved compared with the previous experiment and the performance results of the

experiment above across various ALs and ILs for the inter-process level. There were a total of 1,364k application requests, which is more logical compared with the intra-process and inter-/intra-process results (2,561k and 3,006k, respectively). In addition, the experimental results range from 27% (the shortest time window) to 13% (the largest time window).

		Time Window					
		AL = 2	AL= 5	AL = 5	AL = 10	AL = 10	AL = 20
		IL = 5	IL= 5	IL= 10	IL= 10	IL= 20	IL= 20
Inter	% Average Intrusive Requests	27	21	21	17	17	13
	Total Requests	1,364 k					
	Intrusive ≤ 10% (# users)	4	4	4	8	8	29
	10% < Intrusive ≤ 15%	1	10	10	16	16	29
	15% < Intrusive ≤ 20%	7	16	16	35	35	12
	Intrusive > 20%	64	46	46	17	17	6

Table 5-13: Average percentages of intrusive authentication requests for inter-process

On the other hand, Table 5-13 clearly shows the majority of the average users' intrusive requests distribution was more than 20% of the total average users' intrusive requests for the first three time windows. In contrast, the shortest time window (AL = 2 min / IL = 5 min) achieved the worst result due to the majority of the average users' intrusive requests being 27%. Furthermore, it is worth noting that participant 35 achieved 50% intrusive authentication requests for the shortest time window (AL = 2 min / IL = 5 min) and is considered an outlier when compared with the other participants. Conversely, participants 47, 75, 11, and 4 achieved 9%, 9%, 10%, and 10% intrusive authentication requests, respectively. Those participants achieved 50%, 71%, 40%, and 100% intrusive authentication requests, respectively, without applying the median concept to save the number of application access. One of the reasons for this result could be that WhatsApp was the most-used application for these participants, which means the users made a number of interactions within the WhatsApp application for a long time with access to only one application. Interestingly, these participants (4, 11, 47, and 75) achieved better results for intra-process access at 5%, 5%, 10%, and 17% and 5%, 6%, 9%, and 16% at the intra-/inter-process level, respectively.

Table 5-14 demonstrates the results of grouping the participants under the different time windows for high, medium and low usage. It is apparent from Table 5-14 that the approach of categorising the users into three groups of usage led to better performance and the percentage of intrusive authentication requests decreased remarkably, from 27% to 22% for the shortest time window (AL = 2 min / IL= 5 min). The number of intrusive requests was also reduced to half or

more for each time window for the high usage group. In general, very little enhancement is noticed for the high usage group compared with the medium and low usage groups.

		Time Window – Inter					
		AL = 2	AL = 5	AL = 5	AL = 10	AL = 10	AL = 20
		IL = 5	IL= 5	IL= 10	IL= 10	IL= 20	IL= 20
High Usage	% Average Intrusive Requests	22	18	18	15	15	12
	Total Requests	833,679					
	Intrusive ≤ 10% (# users)	3	3	3	6	6	13
	10% < Intrusive ≤ 15%	1	7	7	7	7	8
	15% < Intrusive ≤ 20%	6	7	7	11	11	5
	Intrusive > 20%	17	10	10	3	3	1
Medium Usage	% Average Intrusive Requests	29	23	23	18	18	12
	Total Requests	260,468					
	Intrusive ≤ 10% (# users)	1	1	1	2	2	9
	10% < Intrusive ≤ 15%	0	1	1	3	3	12
	15% < Intrusive ≤ 20%	1	4	4	14	14	2
	Intrusive > 20%	22	18	18	5	5	1
Low Usage	% Average Intrusive Requests	31	22	22	19	19	15
	Total Requests	270,532					
	Intrusive ≤ 10% (# users)	0	0	0	0	0	7
	10% < Intrusive ≤ 15%	0	2	2	6	6	9
	15% < Intrusive ≤ 20%	0	5	5	10	10	5
	Intrusive > 20%	25	18	18	9	9	4

Table 5-14: Average percentages of intrusive authentication requests for inter-process

5.4 Discussion

In this study, only 11 applications were selected for consideration with a limited number of user actions, which would be highly likely to lose interactions, causing

the loss of many biometric samples. In addition, 47 actions were collected and categorised as high risk (35%), medium risk (47%), low risk (13%) and no risk (4%). With this in mind, the majority of these actions were considered high and medium risk (83%), which, in turn, means identity confidence should be higher in order to exceed the threshold and access the required service. In addition, the experimental results showed that the majority of intrusive requests came from high-risk actions. Despite previous challenges, the experimental results for the intra-/inter-process and intra-process only for the 76 participants were promising across the various ALs and ILs considered, as demonstrated in Table 5-15, together with the worst and best performing time windows for each access level. It is clear from the table that the larger AL/IL time windows led to fewer intrusive authentication requests. The reason for the larger time windows outperforming the shorter time windows could be that a high number of user interactions with a mobile phone leads to the collection of many more biometric samples, thereby raising the identity confidence level.

Furthermore, this study highlights the clear effect of AL value on the average intrusive authentication. Likewise, the degradation function was significantly affected in terms of the total confidence level, as this automatically dropped. This is logical if there were no biometric samples collected or the quality of the modality was poor, especially with the shorter time windows. A further point to be noticed in these results is that the vast majority of intrusive requests came from high-risk actions and very few from medium-risk actions, while there was full transparency for low-risk actions. With regard to the system's robustness and users'

convenience, a short time window is likely to lead to a large percentage of intrusive authentication requests, which could become a problem, thereby disturbing legitimate mobile users. As a result, short time windows would lower the security of the system, which might, in turn, allow an imposter to access a service.

	Intra + Inter	Intra	Inter
Total Requests	3,006 k	2,561 k	1,364 k
Least Effective Time Window	AL = 2 min / IL = 5 min	AL = 2 min / IL = 5 min	AL = 2 min / IL = 5 min
% Intrusive Requests	18	15	27
Most Effective Time Window	AL = 20 min / IL = 20 min	AL = 20 min / IL = 20 min	AL = 20 min / IL = 20 min
% Intrusive	6	5	13

Table 5-15: Average percentages of intrusive authentication requests for inter-process

To consider this in more detail, further investigation was undertaken in order to explore how low usage would affect the total percentage of users' intrusive authentication requests. This was achieved by classifying the 76 participants into different types of users to gain greater insight into optimising the performance results and determining whether a particular grouping of time windows would perform better with a particular type of usage. Classifying participants into three groups of usage indicated a notable improvement and achieved promising

experimental results with regard to intrusive authentication requests compared with those previously reported in the first experiment for all differing AL/IL timings, from the shortest time window (AL = 2 min / IL = 5 min) to the longest time window (AL = 20 min / IL = 20 min). As shown in Table 5-16, the results for the three usage groups underline the evidence for the effect of low user usage on the total average intrusive authentication requests for the time window selected. One possible reason for this could be that there is a suitable time window for each group of usage and, therefore, a high probability of gathering biometric samples when the user interacts with his/her mobile device and the degradation function is not recalled to reduce the identity confidence level when the device is inactive for very short intervals.

To conclude, the experimental results highlight that the proposed approach achieved a desirable level in terms of applying a transparent authentication system to intra-process security. As a result, this system would, in turn, enable control of the overall authentication process, thereby enabling a continuous and non-intrusive authentication approach.

Usage Type	Comparison	Intra + Inter	Intra	Inter
High	Total Requests	2,045 k	1,772 k	833,679
	Least Effective Time Window	AL = 2 min / IL = 5 min	AL = 2 min / IL = 5 min	AL = 2 min / IL = 5 min
	% Intrusive	12	10	22
	Most Effective Time Window	AL = 20 min / IL = 20 min	AL = 20 min / IL = 20 min	AL = 20 min / IL = 20 min
	% Intrusive	3	2	12
Med	Total Requests	464,869	396,640	260,468

Usage Type	Comparison	Intra + Inter	Intra	Inter
	Least Effective Time Window	AL = 2 min / IL = 5 min	AL= 2 min / IL = 5 min	AL = 2 min / IL = 5 min
	% Intrusive	21	18	29
	Most Effective Time Window	AL = 20 min / IL = 20 min	AL = 20 min / IL = 20 min	AL = 20 min / IL = 20 min
	% Intrusive	7	6	12
Low	Total Requests	496,096	392,795	270,532
	Least Effective Time Window	AL = 2 min / IL = 5 min	AL = 2 min / IL = 5 min	AL = 2 min / IL = 5 min
	% Intrusive	22	18	31
	Most Effective Time Window	AL = 20 min / IL = 20 min	AL = 20 min / IL = 20 min	AL = 20 min / IL = 20 min
	% Intrusive	9	8	15

Table 5-4: Average percentages of intrusive authentication requests for inter-process

Chapter Six

Investigation of the Impact Of Modalities on the System

6 Investigation of the Impact of Modalities on the System

6.1 Methodology of Experiment 4

The main aim of the fourth experiment was to investigate the impact of each modality on overall system performance. A wide range of biometrics were used in this research: facial, fingerprint, voice and iris recognition and keystroke, behavioural and linguistic profiling. Time windows of AL = 5 min / IL = 5 min and AL = 10 min / IL = 10 min were selected at the intra- and inter-process access levels in order to test the effects and examine the impact of the biometric simulation scenarios on the performance of the proposed approach. The reason for choosing the aforementioned authentication time windows was based on the notion that smaller time windows might achieve a balance between security requirements and participants' convenience. Although larger verification time windows could lead to more security threats and misuse when there is a large amount of time in which to check the identity confidence level and the user's biometric samples, these time windows would enhance usability.

In order to examine the impact of each modality, three types of experiment were conducted; the code was run without the selected modality and the total intrusive authentication requests were calculated and compared with the overall system performance each time. Based on the experimental results for an individual modality, a combination of the single modality with the greatest impact was selected to test the effect of two modalities on the overall system. Finally, a combination of three modalities was selected to test their combined effect on the

overall system based on the previous experiment. This chapter then continues by discussing the impact of individual biometrics on overall performance system.

6.2 Experiment 4: Impact of Biometric Modalities on Overall System Performance

6.2.1 Introduction

In this experiment, further investigation was required to test the effect of a single biometric modality on overall system performance. As previously mentioned, a simulated scenario in this research has been applied for generating biometric samples with a wide range of biometrics were used in this research: facial, fingerprint, voice and iris recognition, as well as keystroke, behavioural and linguistic profiling. Table 6.1 conducted based on which biometric might be able to capture when the mobile user interact with his/her mobile. For instance, if a user uses a mobile phone to write a message or email, the biometric might be able to capture keystroke samples. Table 6.1 displays further details with regard to the 47 user actions collected and matched with a simulated biometric technique. As presented in this table, the vast majority of user interactions were associated with face and iris recognition techniques: nearly 81% (39 user actions from a total of 47). For this reason, this was the main effect on overall system performance.

No.	Action Name	Face	Iris	Keystroke	Linguistic	Voice
1	Make a call	×	×	×	×	✓
2	Receive a call	×	×	×	×	✓
3	Read an SMS message	✓	✓	×	×	×
4	Send an SMS message	✓	✓	✓	✓	×
5	Download a file	✓	✓	×	×	×
6	Search on YouTube	✓	✓	✓	✓	×
7	Receive a text message	✓	✓	×	×	×
8	Receive an image message	✓	✓	×	×	×

No.	Action Name	Face	Iris	Keystroke	Linguistic	Voice
9	Receive an audio message	✓	✓	×	×	×
10	Receive a video message	✓	✓	×	×	×
11	Receive a contact card	✓	✓	×	×	×
12	Receive a location	✓	✓	×	×	×
13	Receive a free call (voice/ video)	×	×	×	×	✓
14	Receive a PDF file	✓	✓	×	×	×
15	Send a text message	✓	✓	✓	✓	
16	Send an image message	✓	✓	×	×	×
17	Send an audio message	✓	✓	×	×	×
18	Send a video message	✓	✓	×	×	×
19	Send a contact card	✓	✓	×	×	×
20	Send a location	✓	✓	×	×	×
21	Make a free call (voice/video)	×	×	×	×	✓
22	Send a PDF file	✓	✓	×	×	×
23	Search	✓	✓	✓	✓	×
24	Watch a video	✓	✓	×	×	×
25	Download an app	✓	✓	×	×	×
26	Update an app	✓	✓	×	×	×
27	Send an email	✓	✓	✓	✓	×
28	Read an email	✓	✓	×	×	×
29	Make a free voice call	×	×	×	×	✓
30	Make a free video call	×	×	×	×	✓
31	Receive a free voice call	×	×	×	×	✓
32	Receive a free video call	×	×	×	×	✓
33	Receive a text message	✓	✓	×	×	×
34	Receive an image message	✓	✓	×	×	×
35	Receive a sound message	✓	✓	×	×	×
36	Receive a location	✓	✓	×	×	×
37	Send a free text message	✓	✓	✓	✓	×
38	Send a free image message	✓	✓	×	×	×
39	Send a free sound message	✓	✓	×	×	×
40	Send a location	✓	✓	×	×	×
41	Delete a message	✓	✓	×	×	×
42	Upload an image	✓	✓	×	×	×
43	Upload a video	✓	✓	×	×	×
44	Take a photo	✓	✓	×	×	×
45	Record a video	✓	✓	×	×	×
46	Save a photo	✓	✓	×	×	×
47	Save a video	✓	✓	×	×	×

Table 6-1: User actions matched with a biometric technique

As depicted in Figure 6-1, the majority of biometric samples generated were from facial recognition and iris recognition (81%) and the remainder were divided between the other modalities. Two time windows (AL = 5 min / IL = 5 min and AL = 10 min / IL = 10 min) were selected at the intra- and inter-process access levels

in order to test the effect and provide further understanding of whether this would affect overall system performance.

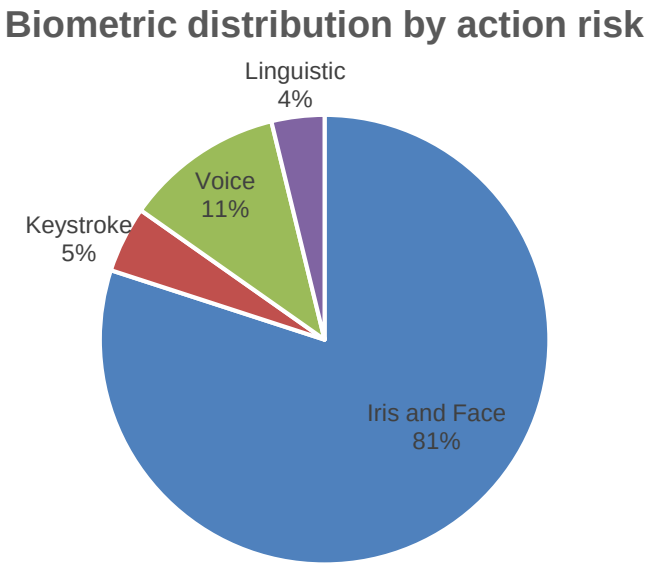


Figure 6-1: Biometric distribution by action risk

6.2.2 Absence of a Single Modality

Table 6-2 presents the experimental results for the total intrusive authentication requests when testing the absence of a single modality in addition to the previous experiments regarding all modalities across two different time windows: AL = 5 min / IL = 5 min and AL = 5 min / IL = 10 min. In this table, it is clear that there is no effect when finger, keystroke, linguistic, or voice is removed from the total biometric calculation. This was as expected and was accepted, as only 20% of the collected user actions were related to these modalities across all the participants, as previously mentioned in section 6.2.1. The most surprising aspect of this experiment was the significant positive difference in the absence of

behavioural profiling compared with all the biometrics in the experiment (by 1%, ranging from 13% to 12%). Turning now to the experimental evidence for the effect of the absence of iris or face recognition, there was a notable increase in the total intrusive authentication requests of 2% and 3% at AL = 5 min / IL = 5 min and AL = 5 min / IL = 10 min, respectively; this was envisaged to be the case, given that the majority of the user actions collected were through face and iris recognition (nearly 80%).

In terms of group usage, the results were in line with the other experiments and showed a substantial improvement in decreasing the number of intrusive authentication requests, as apparent in Table 6-2. For the high usage group, the effect of the absence of iris or face recognition showed the same results but a further point to be noticed is that the results for the absence of behavioural profiling were not affected. However, the change was clear for the medium and low usage groups, which showed a reduction of 1%. The reasons for that might be the high number of user actions for both modalities (39 actions), which suggests that facial and iris recognition might affect the total intrusive authentication requests.

		Time Window	Overall	Without Iris	Without Face	Without Finger	Without Keystroke	Without Behavioural	Without Linguistic	Without voice
All		5/5	13	15	15	13	13	12	13	13
		5/10	13	16	16	13	13	12	13	13
Group Usage	High	5/5	7	11	11	7	7	7	7	7
		5/10	7	12	12	7	7	7	7	7
	Medium	5/5	15	17	17	15	15	14	15	15
		5/10	15	18	18	15	15	14	15	15
	Low	5/5	17	19	19	17	17	16	17	17
		5/10	17	19	19	17	17	16	17	17

Table 6-2: Total intrusive authentication requests – absence of a single modality

Figure 6-2 shows the user intrusive request distribution regarding the impact of the absence of a single modality, in addition to the previous experiments for all the modalities across the different time windows: AL= 5 min / IL = 5 min and AL = 5 min / IL = 10 min. It is clear that, when removing iris and face recognition, respectively, the total intrusive requests increased from 2% to 3%. For instance, nine participants (3, 4, 16, 28, 43, 47, 53, 65 and 71) achieved a high intrusive requests percentage, ranging from 5% to 9%, compared with the experiment for all the biometrics at AL = 5 min / IL = 5 min. Interestingly, three participants (26, 58 and 69) were not affected by the removal of iris or face recognition and

achieved the same results. At the behavioural profiling stage, the results were very close and sometimes achieved better outcomes, as the median for all the participants was 12% and 13% for total intrusive requests at the stage of using all the biometrics, whereas the median was 15% at the iris and face recognition stage. For instance, 19 participants (13, 15, 23, 25, 30, 31, 33, 36, 38, 43, 44, 46, 51, 54, 58, 61, 66, 69 and 70) achieved a 1% reduction in their total intrusive authentication requests when testing the absence of the behavioural proofing modality.

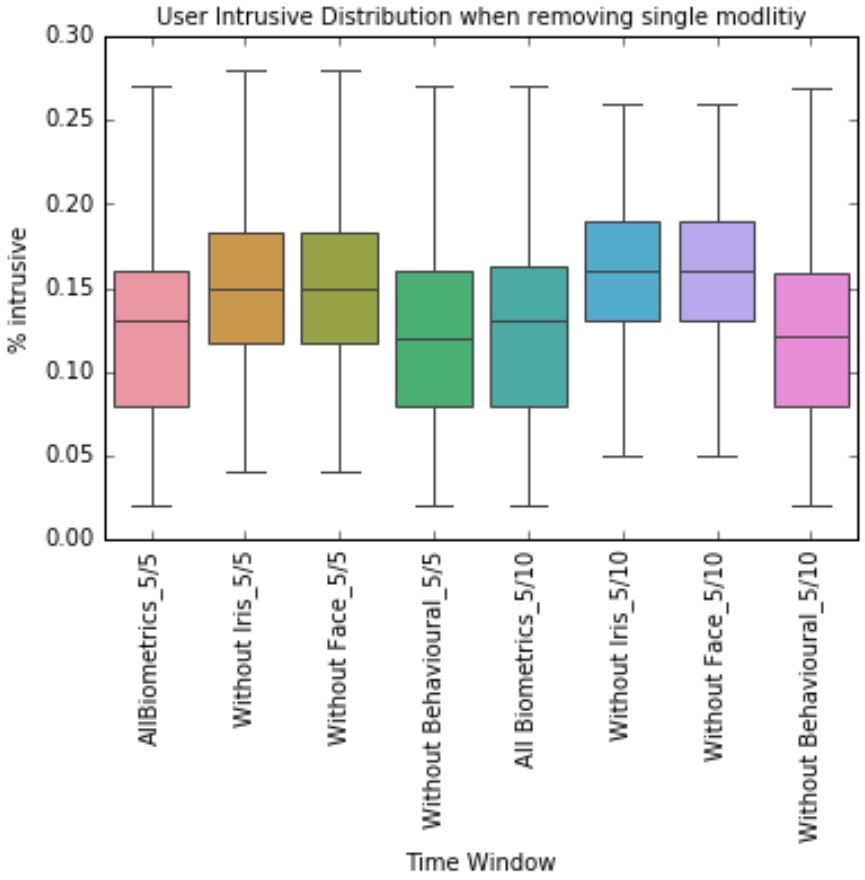


Figure 6-2: User intrusive requests distribution – impact of the absence of a single modality

On the other hand, at AL = 5 min / IL = 10 min, the experimental results were almost identical but with some slight changes, such as to the median. The median ranged from 12% at the behavioural profiling stage to 16% at the face and iris recognition stages, respectively. In this case, the large time window for updating the confidence level did not have a positive effect, as the results have shown.

In this context, participant 4 (a high active user) was selected to examine the difference between the impact of the absence of a single modality and all the biometrics for a series of user actions during a specific time of day. It is apparent from Figure 6-3 that there is a slight difference when removing iris or face recognition and a decrease by almost 10%. It could be the case that this participant benefited from performing lots of actions which related to face or iris biometrics. For instance, the identity confidence level plummeted when there was no user interaction with his/her mobile device at action number 46. This is followed by a sharp rise as a result of the user entering his/her password. However, without the behavioural profiling modality, the result achieved was slightly better and identical.

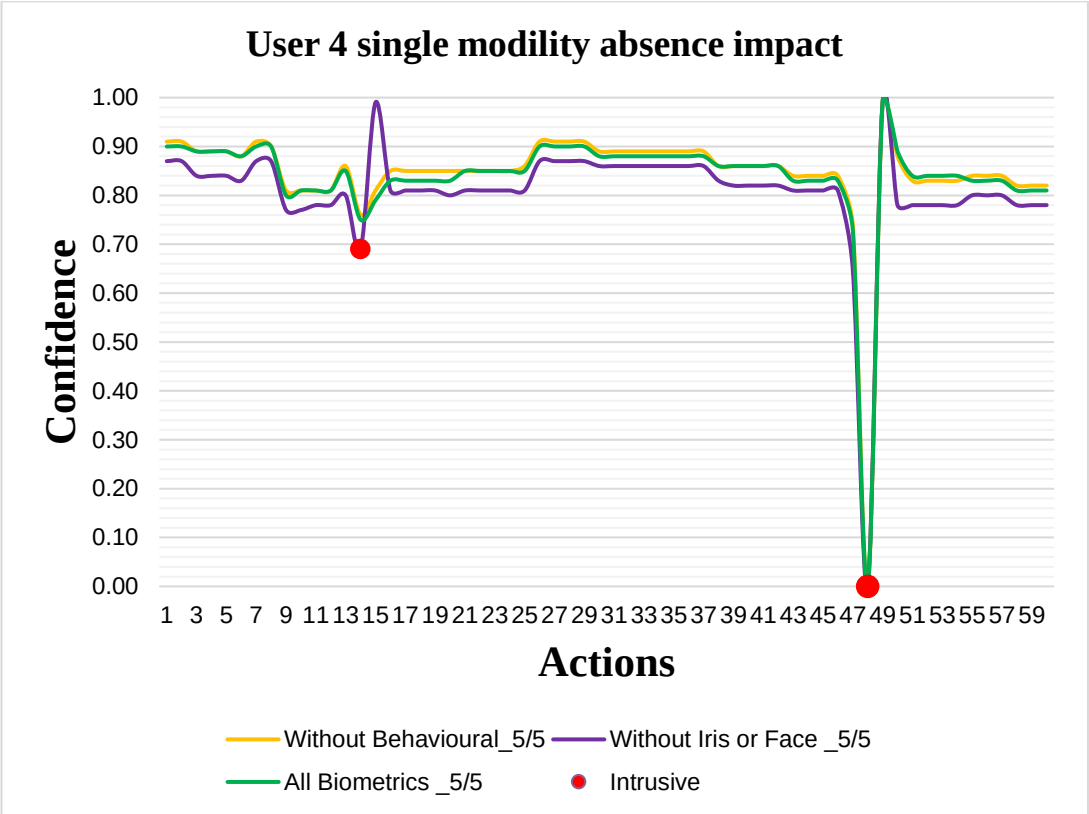


Figure 6-3: User 4 – impact of the absence of a single modality

6.2.3 Absence of Two Modalities

In this experiment, two modalities were selected to test the impact of their absence on overall system performance, as summarised and presented in Table 6-3. The experimental results for the total intrusive authentication requests were considered to investigate the impact of the absence of two modalities, in addition to the previous experiments regarding all modalities across the different time windows: AL = 5 min / IL = 5 min and AL = 5 min / IL = 10 min. As seen in Table 6-3, there is a sharp rise in total intrusive authentication requests in the absence of both iris and face recognition by more than half the original number (i.e., in the all-biometrics case), which was expected to have been more. A possible explanation for these results may be the lack of adequate biometric samples due

to the majority of the collected user actions being face and iris recognition (nearly 80%).

Despite the improvement in the average for all biometrics and a reduction from 13% to 7% for the high usage group, the total intrusive authentication requests diminished slightly across the different time windows. Interestingly, this was different from the medium and low usage groups, whose rates increased. On the other hand, there was only a 1% increase in the total intrusive authentication requests when removing both the iris recognition and behavioural profiling modalities. This result may be explained by iris recognition only as a single modality increasing the total intrusive authentication requests by nearly 3% and behavioural profiling reducing it by 1%, as shown in Table 6-2. In this case, the findings were to be expected. Interestingly, although face and iris recognition represented the same proportion of user actions collected (nearly 80%), when removing both the face recognition and behavioural profiling modalities, nothing changed with regard to the total intrusive authentication requests.

		Time Window	Overall	Without Iris and Face	Without Iris+ Behavioural	Without Face + Behavioural
All		5/5	13	29	15	13
		5/10	13	29	14	13
Group Usage	High	5/5	7	28	10	7
		5/10	7	28	11	7
	Medium	5/5	15	31	16	15
		5/10	15	31	17	15
	Low	5/5	17	30	18	17
		5/10	17	30	18	17

Table 6-3: Total intrusive authentication requests in the absence of two modalities

Figure 6-4 shows the impact on user intrusive requests distribution of the absence of two modalities, in addition to the previous experiments for all modalities across the different time windows: AL = 5 min / IL = 5 min and AL = 5 min / IL = 10 min. In this figure, it appears that there is a notable effect of the absence of both iris and face recognition for both time windows. For instance, the median for the total intrusive authentication requests was 28% in the case of the absence of both iris and face recognition with a wide gap in relation to other combinations of

biometrics collected, which did not exceed 15%. In addition, nearly 75% of the participants show significantly higher total intrusive authentication requests by at least double when compared with the original. For instance, participants 3, 4, 35 and 42 range from 3% to 39%, 2% to 30%, 20% to 48%, and 7% to 34%, respectively. Interestingly, four participants (2, 17, 58 and 59) show a slight increase in the total intrusive authentication requests, ranging from 23% to 29%, 16% to 19%, 24% to 27%, and 14% to 20%, respectively. One possible reason is that these participants were already classified as low active users.

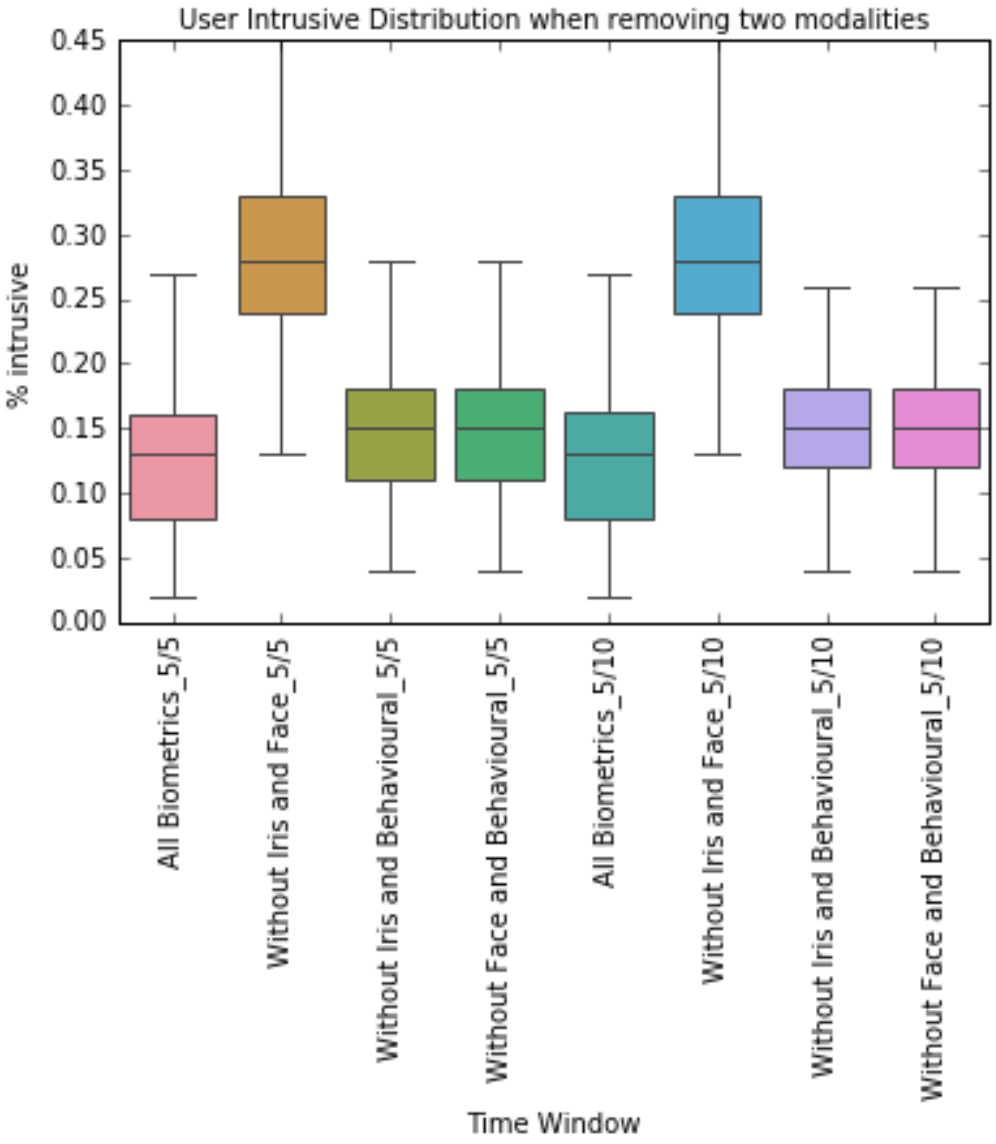


Figure 6-4: User intrusive requests distribution – impact of the absence of two modalities

On the other hand, in the case of iris and behavioural profiling, there was a clear trend showing an increase in total intrusive authentication requests. For instance, six participants (3, 4, 28, 47, 57 and 71) show intrusive authentication requests of almost 5% to 11%, whereas eight participants (2, 17, 23, 26, 30, 36, 46 and 58) show no effect from this change. In addition, it was noticeable that participant 69

changed from 19% to 18%. The reason for this was not clear but this user may not depend on iris or face biometric capturing.

Participant 65 (a medium active user) was then selected to examine the difference between the impact of the absence of two modalities and all biometrics for a series of user actions during a specific time of day. It is apparent from Figure 6-5 that the absence of both iris and face recognition caused fluctuation, resulting in a high percentage of intrusive authentication requests and the most negative result. It may be that this participant benefited from lots of actions related to face or iris biometrics. On the other hand, without iris and behavioural profiling modalities set between without iris and face recognition and the all modalities due to the impact of iris recognition as shown in the previous figures. For instance, at action 41, the identity confidence level decreases because the user has not used his/her mobile for a while and the degradation function was recalled. It is clear that there is a gap between the all-biometrics scenario and iris and face recognition of at least 35%. However, a slight change occurred when removing iris recognition and behavioural profiling. Another observation relating to Figure 6-5 is that there might be times when the identity confidence level does not need intrusive requests due to the action being low or no risk.

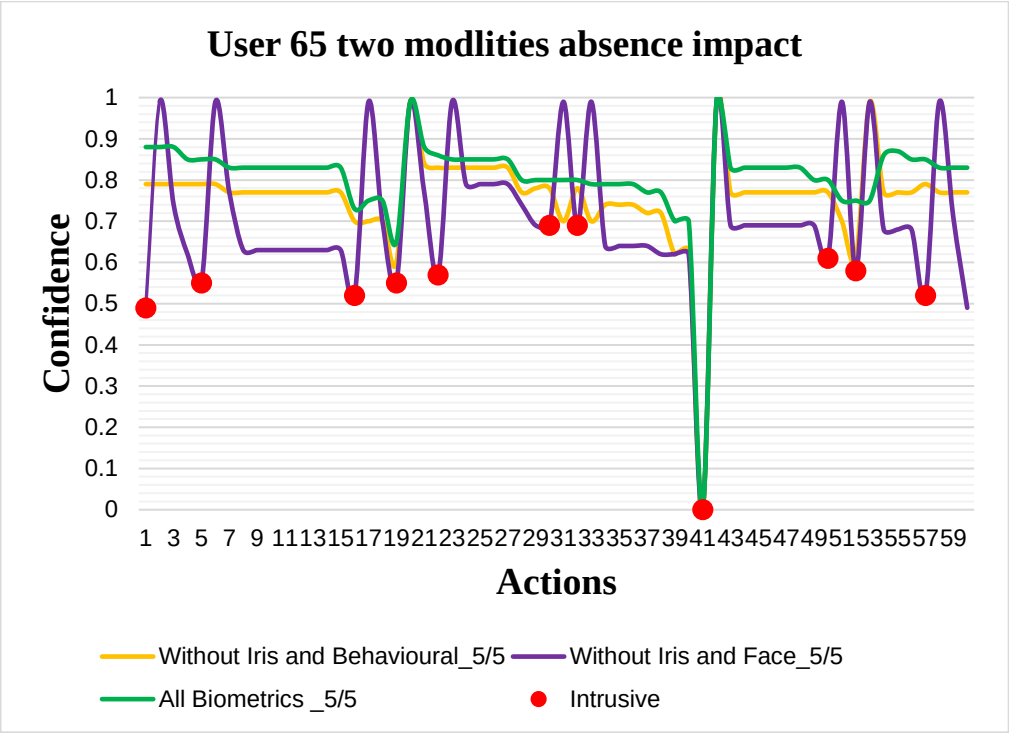


Figure 6-5: User 65 – impact of the absence of two modalities

6.2.4 Absence of Three Modalities

The experimental results for the total intrusive authentication requests used to investigate the impact of the absence of three modalities in addition to the previous experiments involving all modalities across different time windows (AL = 5 min / IL = 5 min and AL = 5 min / IL = 10 min) are summarised and presented in Table 6-4. As shown in the table, the impact of the absence of iris and face recognition is clear, as their effect progressively increases with both behavioural profiling and voice recognition. For instance, in the absence of iris, face and behavioural profiling, the total intrusive authentication requests increase by more than half of those for the all-biometrics experiment (ranging from 13% to 29% at AL = 5 min / IL = 5 min, and to 34% at AL = 5 min / IL = 10 min). This result was expected and accepted due to face and iris recognition, when combined together,

achieving the worst result for the total intrusive authentication requests, as shown in the previous experiment. Interestingly, the total intrusive authentication requests show a slight decrease for the high usage group, which demonstrates a notable improvement compared with the medium and low usage groups.

		Time Window	Overall	Without Iris and Face+ Behavioural	Without Iris and Face+Voice
All		5/5	13	29	29
		5/10	13	34	29
Group Usage	High	5/5	7	28	28
		5/10	7	34	28
	Medium	5/5	15	30	31
		5/10	15	35	31
	Low	5/5	17	30	30
		5/10	17	34	30

Table 6-4: Total intrusive authentication requests – impact of the absence of three modalities

Figure 6-6 shows the user intrusive requests distribution for the impact of the absence of three modalities, in addition to the previous experiments involving all modalities across two different time windows: AL = 5 min / IL = 5 min and AL = 5

min / IL = 10 min. The figure shows that the effect becomes more noticeable with the absence of iris and face recognition and that they play an important role in raising the total intrusive authentication requests across the different time windows (AL = 5 min / IL = 5 min and AL = 5 min / IL = 10 min). For instance, the median for the total intrusive authentication requests was 28% in the case of iris and face recognition and there is a wide gap in relation to the other types of biometrics collected, which did not exceed 14%.

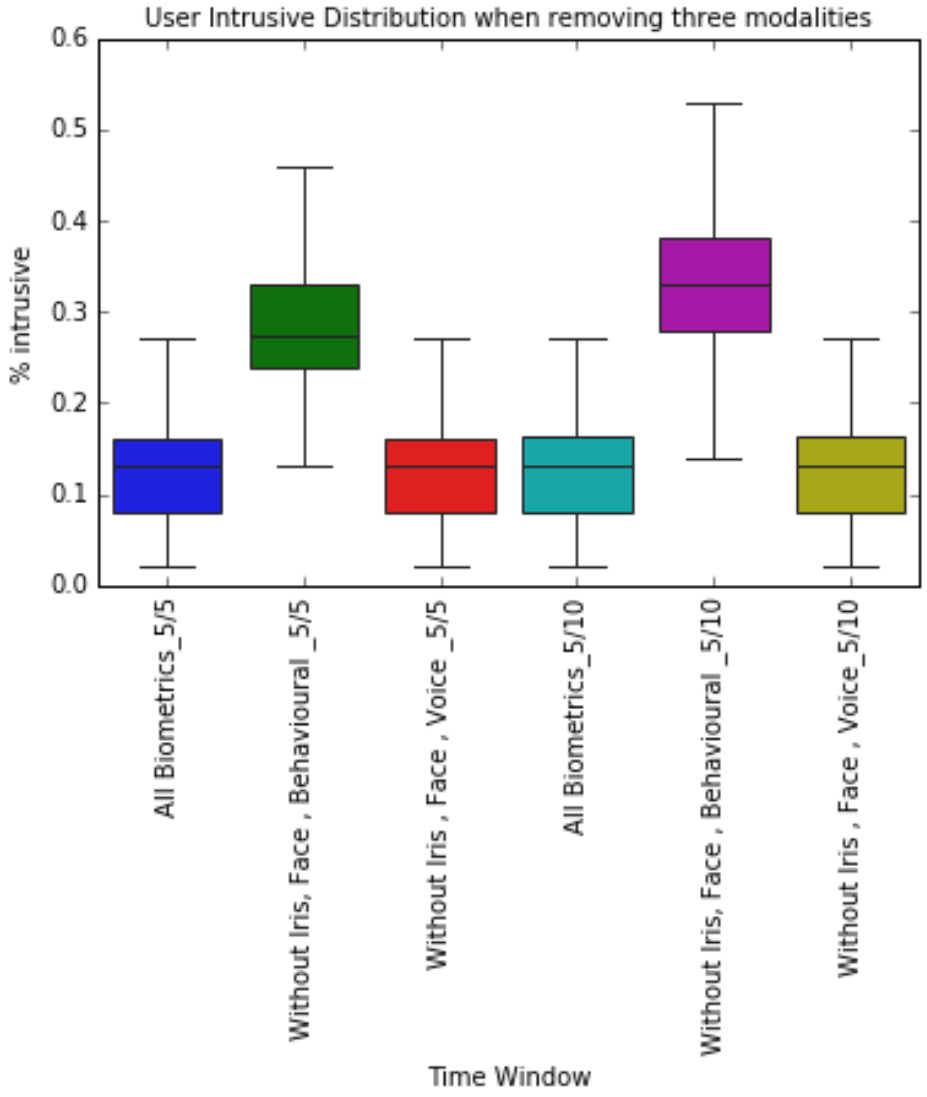


Figure 6-6: User intrusive requests distribution – impact of the absence of three modalities

In addition, nearly 75% of the participants show significantly higher total intrusive authentication requests by at least twofold in comparison with the original results. For instance, participants 3, 4, 35 and 42 range from 3% to 39%, 2% to 30%, 20% to 48%, and 7% to 34%, respectively, which were the same results as those relating to the absence of two modalities (i.e., iris and face recognition). Likewise, four participants (2, 17, 58 and 59) show a slight increase in the total intrusive authentication requests, ranging from 23% to 29%, 16% to 19%, 24% to 27%, and 14% to 20%, respectively. These individuals were classified as low active users and this may have resulted in a large number of intrusive authentication requests.

Figure 6-7 presents the impact of the absence of three modalities for user 47 (a high usage user). The graph shows that the results for the absence of iris and face recognition modalities continues to lower the user confidence level, which results in a high percentage of intrusive requests. More specifically, the removal of behavioural and voice modalities did not make a difference to the overall results. For the 59 user actions plotted, only one identity verification was required (at user action number 17) when all the biometrics techniques were applied in the case that there was no user interaction with his/her mobile. However, there were 10 intrusive authentication requests when the iris and face recognition modalities were removed. To conclude, the greater the number of modalities removed, the lower the user confidence level, which results in a higher percentage of intrusive authentication requests.

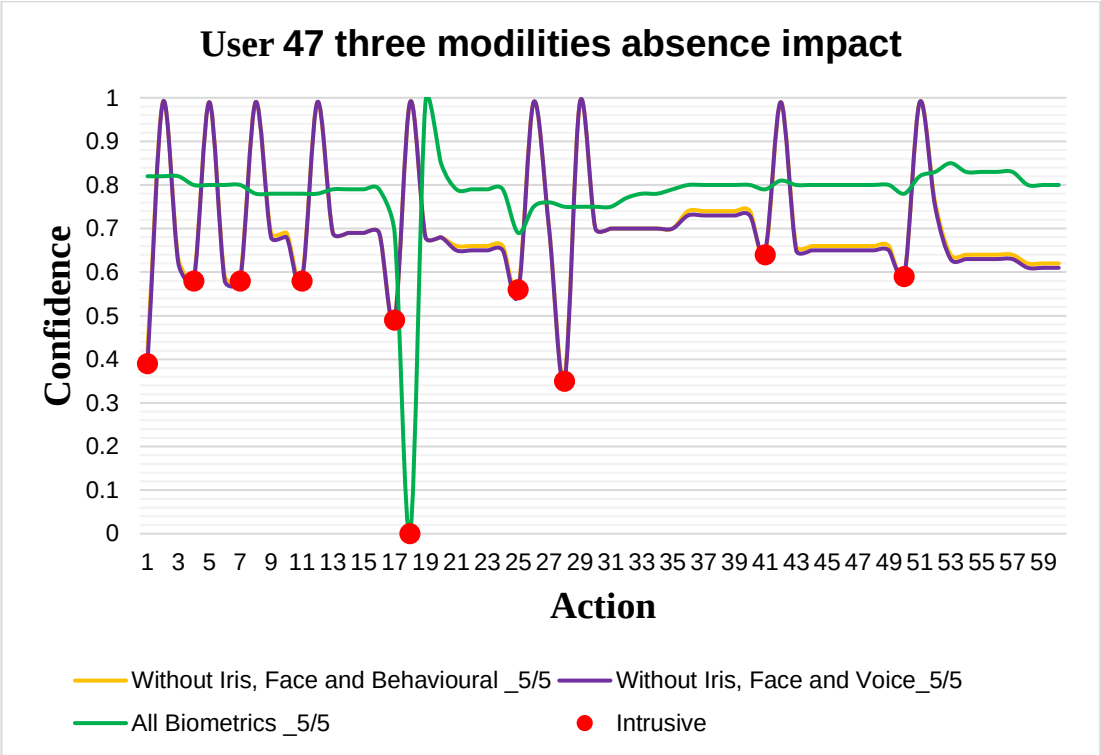


Figure 6-7: User 47 – impact of the absence of three modalities

To conclude, the impact of iris and face recognition on the overall system is clear for all three types of absence (single modality, two modalities, and three modalities). As previously mentioned, the vast majority of user interactions were associated with face and iris recognition techniques (nearly 81%; that is, 39 user actions from the total of 47). For this reason, this was the main effect on overall system performance.

7 Conclusions and Future Work

User authentication on mobile devices has become an increasingly important consideration. After the point-of-entry authentication stage at the beginning of a session, using modalities such as a PIN or password, the user of the device can perform almost all tasks, with different risk levels, without having to re-authenticate periodically to re-validate the user's identity. Furthermore, the current point-of-entry authentication mechanisms consider all applications on a mobile device to have the same level of importance and maintain a single level of security for all applications, thus not applying any further access control rules. As a result, with the rapid growth of mobile devices for use in our daily lives, securing the sensitive data stored upon them makes authentication of paramount importance.

The main objective of this research was to propose and develop an intelligent transparent authentication framework for intra-process security for mobile applications that both fulfils security obligations and provides continuous protection to ensure the validity of the current user. This objective was achieved by first presenting a comprehensive review and analysis of the literature on transparent authentication systems for mobile device security. This research then presented a taxonomy of mobile applications data with justifications and introduced an innovative mobile applications data risk assessment model, called MORI (Mobile Risk), which determines the risk level for each process on a single application. Finally, this approach was implemented to perform authentication continuously and conveniently for mobile applications.

This final chapter summarises and concludes the work of this thesis by outlining the research contributions and the main achievements of the research project. The chapter then discusses the shortcomings of the research, its limitations and the obstacles encountered for further investigation and research. Finally, the chapter identifies several potential research directions and considers future work within the mobile device security field and how the research could proceed from this point.

7.1 Contributions and Achievements of the Research

As originally outlined in chapter one, the research aims and objectives have been achieved with a series of experimental studies. These studies have led to the introduction of a framework for a transparent, intra-process authentication approach for mobile applications. In addition, a number of peer-reviewed papers have been produced and presented at conferences and published in internationally recognised journals during the course of this research, which suggests that the research is deemed to have made positive contributions to the field of user authentication and specifically to the biometric identity verification domain.

The following key contributions have been made by this research by meeting the following objectives of this study project:

- **Objective 1:** To review the importance of mobile devices and the evolution of mobile applications and fully investigate the leading current authentication approaches. The research project established, by reviewing the popularity of mobile devices, our increasing reliance upon them and

the importance of the security of these devices. The work then provided an overview of some of the currently provided authentication technologies and reviewed biometric authentication from a number of perspectives, including its system components, requirements, techniques, performance measures and fusion. The relevant chapter ended with the current authentication mechanisms for mobile devices and the security issues involved (chapter two).

- **Objective 2:** To investigate the current state-of-the-art literature on transparent and continuous authentication for mobile device security. This study briefly outlined the concept of a transparent authentication system and the need for it. This was followed by an exhaustive literature review of the existing research in this domain on continuous and transparent authentication systems for mobile devices and a comparative summary of each category was provided. Building upon this, the discussion ended by identifying the gap that exists in the literature by highlighting the security issues and authentication alternatives for modern mobile devices and the need for a new security mechanism which can provide continuous and transparent protection for better securing mobile devices (chapter three).

- **Objective 3:** To produce a novel mobile applications data taxonomy by investigating and studying the risk for each process within an application in order to explore the level of user action risk. This research project drew attention to the need to study the risk relating to each process within an

application and explained the need for intra-process security for mobile devices through examples of different types of applications. The research project then introduced a novel mobile applications data risk assessment model. A taxonomy of mobile applications data was then presented, with justifications, by studying the risk for each process within 10 of the most popular mobile categories, which were analysed to gain a comprehensive understanding of the various risk levels associated with the user actions on those applications. This research shows that there is sensitive information beyond the point of entry and that the risks change within applications (chapter four).

- **Objective 4:** To propose an innovative risk assessment model for mobile applications data, called MORI (Mobile Risk), which can be used to determine the risk level for each process on a single application. This research presented a generic risk assessment model for mobile applications data with a particular focus on analysing and producing a risk matrix that might help move the access control system from the application level to the intra-process application level, based on the risk relating to the user action being performed as part of the processes (chapter four).

- **Objective 5:** To develop user action determination software in order to create a real dataset to utilise in the study experiments. In order to investigate the feasibility of building a transparent and continuous biometric-based system, it was necessary to collect samples of genuine

user interactions with their mobile devices/apps based upon a substantive period of real-world use (noting that such samples would be based upon data that are naturally logged by apps on the devices anyway, and so the research would not be gathering information that is not already collected; it would, however, be applying it for an additional purpose). As such, it was proposed to enlist participants and collect log data from them after one month of normal device usage. It should be noted that these data are anonymous and that participation did not require the participants to do anything other than use their devices as normal. This experiment collected the sort of data that are logged routinely, such as a time stamp of the application used by the participant and the name of the user action (read, send, etc.), but this experiment did not collect such information as passwords, messages, etc. As a result, a significant number of real participants (76) in completely uncontrolled conditions were assembled and 47 user actions were gathered from 12 selected applications during at least one month of normal device usage (chapter five).

- **Objective 6:** To conduct a series of experiments aimed at investigating the feasibility of the proposed system. This study conducted the following set of experiments: a biometric transparent authentication system on intra- and inter-process, intra-process (i.e., within app) only and inter-process (i.e., only app) only access across different time windows. For each experiment, all participants were classified into three usage levels (low, medium and high) due to the observation that some users performed an

insufficient number of activities on their device and, therefore, showed a high level of intrusive authentication requests. As a result, there was a need to investigate whether a specific combination of time windows would perform better with a specific type of user, an approach which was shown to achieve better results compared with the first experiment (chapter five).

- **Objective 7:** To investigate the impact of specific biometric modalities on overall system performance in terms of three types of modality: single, two, and multimodalities. In this research study, a wide range of biometrics were simulated and further investigation was required to test the effect of a single biometric modality on overall system performance (chapter six).

7.2 Limitations of the Research Project

Although the research programme objectives have been met, a number of limitations and issues have been identified as being linked to the work progress and findings and need to be considered. The key limitations of this study are briefly listed below.

1. This research study collected 47 user actions from only 12 selected applications, in order to protect the users' privacy and not ask participants to root their device. The data collected for analysis might be insufficient and collecting data on more user actions from more applications would have provided a richer and more comprehensive set of user interactions from the extracted log files for each participant, which might have lost biometric samples. Therefore, the experimental results might have been

further improved if many more user actions had been collected from a greater number of applications.

2. EERs previously published in the literature were utilised as simulative biometric scenarios and input in all the experiments. This was due to the difficulty of finding applicable open source biometric classifiers, as this research study was managed and performed by a PhD researcher and was limited in terms of duration, timeframe and resources. As a result, this did not enable the presentation of real-time mobile usage and consideration needs to be given to this issue.
3. The proposed risk assessment model for mobile applications data was not tested and evaluated across different types of participants in a real environment through surveys, focus groups or interviews. As a result, there is a need for further analysis to be pursued to appreciate the practical usefulness of the proposed risk assessment model and to gain greater insight into the effectiveness of this model.
4. The user actions determination technique used in this study relied upon data collected from databases by utilising SQLite from each selected application.

7.3 Suggestions and Scope for Future Work

Despite the limitations of the research project presented in the previous section, this research project has advanced and improved the field of user authentication for smartphones in general and mobile application security and usability in particular. As with any research, there are a number of opportunities for future work and enhancement in further investigation within the area of user

authentication on mobile applications. This presents a significant opportunity to take the proposed research to the next level and further substantiate intra-process security as an improvement upon traditional methods of mobile device security.

The details of these research opportunities are highlighted below:

1. Studying the risk relating to each process within an application has not been investigated apart from this research, which has a solid foundation in this area of study. Therefore, consideration should be paid to this area of research in order to enhance and improve the security of mobile applications data and user convenience.
2. There is a clear need for additional investigation into techniques of user action determination that would lead to providing more insight into system performance.

7.4 Future of User Authentication on Mobile Devices

With the rapid growth in the use of smartphones in our daily lives, securing the sensitive data stored upon them makes authentication of paramount importance. In particular, smartphones are used to perform activities which are considered sensitive and confidential, and the risks are high in the event of the loss of sensitive data or privacy breaches. In addition, after the point of entry, by using techniques such as a PIN or password, the user of a device can perform almost all tasks, with different risk levels, without having to re-authenticate periodically to re-validate the user's identity. Furthermore, the current point-of-entry

authentication mechanisms consider all applications on a mobile device to have the same level of importance and thus do not apply any further access control rules. Unlike previous work, this research argues that within a single mobile application there are different processes operating on the same data but with differing risks attached. The unauthorised disclosure or modification of mobile data has the potential to lead to a number of undesirable consequences for the user. Thus, there is no single level of risk associated with a given application and the risk level instead changes during use. Accordingly, there is a need to suggest a method that can be applied continuously and transparently (i.e., without obstructing the user's activities) to authenticate legitimate users, which is maintained beyond the point of entry, without the explicit involvement of the user.

To this end, this research project has suggested a new mechanism to address this problem by utilising a transparent and continuous authentication system. This transparent and continuous authentication mechanism provides a basis for the convenient and secure re-authentication of the user and gathers user data in the background without requiring any dedicated activity by regularly and periodically checking user behaviour in order to monitor the protection of the smartphone continuously. Finally, this study has introduced a transparent, intra-process user authentication approach for mobile applications in order to verify whether the authenticated user is the legitimate owner of the mobile device.

This work would help shape the future mobile application security field by ensuring that the right person is allowed to access the right information at the right time. Furthermore, this research study could, in the future, assist research activities to investigate the risks within the application. In addition, a further aspect

that needs to be considered is to understand the nature of the risk to which the data are exposed in order to apply the appropriate protection to those data thereby improving user authentication security. Likewise, this work would help mobile developer to protect mobile and this approach would achieve good levels of usability by utilizing a combination of the device owner's biometrics.

References

1. ABI Research, 2010. ABI Research, World Mobile Applications Market – Advanced Technologies, Global Forecast (2010-2015) available at: http://www.marketsandmarkets.com/Market-Reports/mobile-applications-228.html [Accessed 11th March 2015]
2. Al Abdulwahid, A., Clarke, N., Furnell, S., & Stengel, I., 2013. A conceptual model for federated authentication in the Cloud. In the 11th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia.
3. Al Abdulwahid, A., Federated Authentication using the Cloud (Cloud Aura), Plymouth university, 2017
4. Aloul, F., Zahidi. S., & El-Haj.j W., 2009. Two factor authentication using mobile phones. IEEE/ACS International Conference on Computer Systems and Applications. IEEE, 641-644.
5. Apple. 2014. Touch ID: Security. Right at your fingertip', Apple website, available at: https://www.apple.com/iphone-6/touch-id/ [Accessed: 17 Nov 2015]
6. Apple, 2017: About Face ID advanced technology available at https://www.apple.com/uk/iphone-x/
7. Apple, 2018 available at https://support.apple.com/en-gb/HT208108
8. Aviv, A.J., Gibson, K., Mossop, E., Blaze, M. & Smith, J.M., 2010. Smudge Attacks on Smartphone Touch Screens, Proceeding in WOOT'10 Proceedings of the 4th USENIX conference on Offensive technologies.

9. Alotaibi, S., Alruban, A., Furnell, S., and Clarke, (2019) N. A Novel Behaviour Profiling Approach to Continuous Authentication for Mobile Applications in the 5th International Conference on Information Systems Security and Privacy at: Prague, Czech Republic.
10. Acien, A., Morales, A., Vera-Rodriguez, R., and Fierrez, J. (2019). MultiLock: Mobile Active Authentication based on Multiple Biometric and Behavioral Patterns. ArXiv preprint arXiv: 1901.10312.
11. Al-Obaidi, F Li, N Clarke, B Ghita, and S Ketab: A multi-algorithmic approach for gait recognition, 17th European Conference on Cyber Warfare and Security, 20-28.
12. Alghamdi, S. J., and Elrefaei, L. A. (2018). Dynamic Authentication of Smartphone Users Based on Touchscreen Gestures. Arabian journal for science and engineering, 43(2), 789-810.
13. Barrera, D., Kayacik H., van Oorschot, P., & Somayaji, A., 2011. A methodology for empirical analysis of Permission-based security models and its application to android. In Proc. of ACM CCS'10.
14. Biometrics Institute .2013. Biometrics Institute Industry Survey, 1-6.
15. Boehm, A., Chen, D., Frank, M., L. Huang, Kuo, C., Lolic, T., & Song, D., 2013. Safe: Secure authentication with face and eyes. In Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE2013 , pp.1-8.
16. Burgbacher, U., & Hinrichs, K., 2014. An implicit author verification system for text messages based on gesture typing biometrics. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, pp.2951-2954.

17. Buriro, A., Crispo, B., and Zhauniarovich, Y., 2017. Please hold on: unobtrusive user authentication using smartphone's built-in sensors. In: 2017 IEEE International Conference on Identity, Security and Behavior Analysis, ISBA 2017.
18. Cai, Z., Shen C., Wang, M., Song, Y., & J, 2013 Mobile authentication through touch-behaviour features. In Biometric Recognition. Springer International Publishing, pp.386-393.
19. Chen, R., Lin, X., & Ding, T. (2012). Liveness detection for iris recognition using multispectral images. Pattern Recognition Letters, 33(12), 1513–1519.
20. Chen, S., Pande, A., & Mohapatra, P., 2014 Sensor-assisted facial recognition : An enhanced bio-metric authentication system for smartphones. In Proceedings of the 12th annual international conference on Mobile systems, applications, and services MobiSys
21. Cheng, B., Zhang, L., Li, X., Huang, Q., & Wang, Y., 2013, SilentSense: Silent user identification via touch and movement behavioural biometrics. In Proceedings of the 19th annual international conference on Mobile computing & networking - MobiCom 13. ACM. Pp.187–190.
22. Chiasson, S., Biddle ,R., & van Oorschot , P., 2007.A Second Look at the Usability of Click-Based Graphical Passwords, in Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07). ACM, pp. 1 – 12.
23. Chrome Info Technologies. 2016. Top 12 Mobile App Development Trends In 2016, available at http://www.slideshare.net/ChromeInfotech/top-12-mobile-app-development-trends-to-come-in-2016 [Accessed 29 March 2016].

24. Chuang, Y. H., Lo, N. W., Yang, C. Y., & Tang, S. W., 2018. A Lightweight Continuous Authentication Protocol for the Internet of Things. Sensors, 18(4), 1104.
25. Clarke N. and Furnell S., 2005. Authentication of users on mobile telephones – A survey of attitudes and practices. Computers & Security 24(7): 519-527.
26. Clarke N., Furnell .S. & Reynolds .P. 2002. Biometric Authentication for Mobile Devices in Proceedings of the 3rd Australian Information Warfare and Security Conference 2002, pp. 61 – 69.
27. Clarke, N. & Furnell, S., 2007, Authenticating mobile phone users using keystroke analysis, International Journal of Information Security, vol. 6, no. 1, pp.1-14, 2007.
28. Clarke, N., & Furnell S., 2007. Advanced user authentication for mobile devices. Computers & Security 26(2): 109-119.
29. Clarke, N., 2011. Transparent user authentication: biometrics, RFID and behavioural profiling, Springer Science & Business Media.
30. Clarke, N., Furnell, S., Lines, B., & Reynolds, P., 2003 Keystroke dynamics on a mobile handset: A feasibility study, Information Management and Computer Security, vol. 11, no. 4, pp.161-166.
31. Clarke, N., Karatzouni, S., & Furnell, S., 2009 Flexible and transparent user authentication for mobile devices, IFIP Advances in Information and Communication Technology, 297/2009, pp.1-12.
32. Cnet, 2018, Galaxy S9 Intelligent Scan favors unlocking ease over security avialbe at https://www.cnet.com/news/samsung-galaxy-s9-intelligent-scan-unlock-favors-ease-over-security/

33. ComScore Reports, 2015. The 2015 U.S. Mobile App Report, available at: https://www.comscore.com/Insights/Presentations-and-Whitepapers/2015/The-2015-US-Mobile-App-Report, [Accessed 24th February 2016].
34. ComScore. 2015. The UK goes mobile: MMX MP, UK, 2015. ComScore Mobile Metrix, UK, March 2015, available at: http://www.comscore.com/Insights/Data-Mine/Mobile-Metrix-Reveals-the-UKs-Top-Smartphone-and-Tablet-Destinations comScore Mobile Metrix in the UK, [Accessed 29 March 2015].
35. Conti, M., Zachia-Zlatea, I., & Crispo, B., 2011, Mind how you answer me! Transparently authenticating the user of a smartphone when answering or placing a call. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. ACM, pp.249-259.
36. Crawford, H.& Renaud, K., 2014 .Understanding user perceptions of transparent authentication on a mobile device, J. Trust Manag., vol. 1, no. 7, pp.1-28.
37. Crawford, H., Renaud, K., Storer, T., 2013. A framework for continuous, transparent mobile device authentication, Elsevier Computers & Security, 39(2).
38. Crawford, Heather Anne, 2012. A framework for continuous, transparent authentication on mobile devices. PhD thesis.
39. Crouse, D., Han, H., Chandra, D., Barbello, B., & Jain, A., 2013, Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data.

40. CSID, 2012.Consumer Survey: Password Habits, A study among American consumers , available at: http://www.csid.com/wpcontent/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf [Accessed 5 March 2016].
41. Data protection centre, 2018 available at http://dataprotectioncenter.com/access-control-2/behavioral-biometrics-will-replace-passwords-by-2022-gartner/
42. Davey, J., 1991. Risk Analysis and Management. Data Protection and Confidentiality in Health Informatics, IOS Press, pp.350-359.
43. De Luca, A., Hang A., Brudy, F., Lindner C., & Hussmann, H., 2012, Touch me once and I know it's you! Implicit authentication based on touch screen patterns, in ACM CHI, pp.987-996.
44. De Marsico, M., Galdi, C., Nappi, M., & Riccio D., 2014, FIRME: Face and Iris Recognition for Mobile Engagement, Image and Vision Computing, vol. 32, no. 12, pp.1161-1172.
45. De Marsico, M., Nappi, M. Riccio, D. & Wechsler, H., 2015 .Mobile Iris Challenge Evaluation (MICHE)-I, biometric iris dataset and protocols. In Pattern Recognition Letters. Elsevier Ltd., pp.17-23.
46. Derawi, M., Nickel, C., Bours, P., & Busch, C., 2010 Unobtrusive user-authentication on mobile phones using biometric gait recognition. In Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on. IEEE, pp.306-311.
47. Draffin, B., Zhu, J., |& Zhang, J., 2014, Keysens: passive user authentication through micro-behaviour modeling of soft keyboard interaction, In Proc. 5th

International Conference on Mobile Computing, Applications and Services, pp.184-201.

48. Drummond, J., 2014. How the Samsung Galaxy S5 fingerprint scanner differs from Apple's Touch ID', iphonehacks.com, available at: http://www.iphonehacks.com/2014/02/samsung.html [Accessed: 24 May 2015]
49. Du, Y., Arslanturk, E., Zhou, Z., & Belcher, C. (2011). Video-Based Noncooperative Iris Image Segmentation. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 41(1),64–74.
50. Elftmann, P., 2006. Secure Alternatives to Password-based Authentication Mechanisms, Lab. for Dependable Distributed Systems, RWTH Aachen Univ.
51. EPIC, 2005. Biometric Comparison Guide, available at: http://epic.org/privacy/surveillance/spotlight/1005/irid_guide.pdf, date accessed: [Accessed 4th June 2015]
52. ENISA. 2006. Risk management: Implementation principles and inventories for risk management/risk assessment methods and tools.pdf
53. Eurobarometer, 2010. Attitudes on data protection and electronic identity in the European Union. , available at: http://ec.europa.eu/public_opinion/archives/ebs/ ebs_335_en.pdf. [Accessed 20th March 2016].
54. Ehatisham-ul-Haq, M., Azam, M. A., Naeem, U., Amin, Y., and Loo, J. (2018). Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. Journal of Network and Computer Applications, 109, 24-35.

55. El Fray, I. (2012, September). A comparative study of risk assessment methods, MEHARI and CRAMM with a new formal model of risk assessment (FoMRA) in information systems. In IFIP International Conference on Computer Information Systems and Industrial Management (pp. 428-442). Springer, Berlin, Heidelberg.
56. ExpressPigeon, 2014. 33 Mind Shattering Email Marketing Statistics You Need to Know In 2014, available at https://expresspigeon.com/blog/2014/01/06/email-marketing-statistics-2014/ [Accessed 8th November 2015]
57. Facebook Statistics, 2015, available at: http://newsroom.fb.com/company-info[Accessed 20 March 2015].
58. Feng T., Yang J., Yan Z., Tapia E., & Shi, W., 2014 Tips: Context-aware implicit user identification using touch screen in uncontrolled environments, in Workshop on Mobile Computing Systems and Applications.
59. Feng, T., Liu, Z., Kwon , K., Shi, W., Carbunar , B., Jiang Y., & Nguyen ,N., 2012 Continuous mobile authentication using touchscreen gestures, in IEEE HST, pp.451–456.
60. Fiegerman, S., 2014. Android now has 1 billion active users, available at: http://mashable.com/2014/06/25/android-one-billion-users/#EmzBSbVfGaqH [Accessed 4th March 2015].
61. Faris, S., Ghazouani, M., Medromi, H., and Sayouti, A. (2014). Information security risk Assessment– a practical approach with a mathematical formulation of risk. International Journal of Computer Applications, 103(8), 36-42.

62. Frank, M., Biedert, R., Ma E., Martinovic, I, & Song, D., 2013 Touchalytics: On the applicability of touchscreen input as a behavioural biometric for continuous authentication, IEEE Trans. Inf. Forensics Security, vol. 8, no. 1.
63. Fridman, L., Weber, S., Greenstadt, R., & Kam, M., 2015 Active authentication on mobile devices via stylometry, application usage, web browsing, and GPS Location. In arXiv preprint arXiv, pp.1-10.
64. Furnell, S., & Clarke, N., 2014. Biometrics: making the mainstream. Biometric Technology Today, pp.5-9.
65. Furnell, S., Clarke, N., 2013. Towards continuous and convenient user authentication. In The Future of Identity: A compilation of research papers from a workshop.
66. Furnell, S., Katsikas, S., Lopez, J. & Patel, A., 2008. Securing Information and Communica-tions Systems: Principles, Technologies, and Applications. Artech House.
67. Filippov, A. I., Iuzbashev, A. V., & Kurnev, A. S. (2018, January). User authentication via touch pattern recognition based on isolation forest. In 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (pp. 1485-1489). IEEE.
68. Gafurov, D., 2004 Performance and security analysis of gait-based user authentication. PhD thesis, Universitas Osloensis.
69. Gartner, 2013. Gartner Says Worldwide PC, Tablet and Mobile Phone Combined Shipments to Reach 2.4 Billion Units in 2013', available at: http://www.gartner.com/newsroom/id/2408515 [Accessed 19 December 2015].

70. Gupta, S., Buriro, A., & Crispo, B. 2018. Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access. Mobile Information Systems.
71. Gritzalis, D., Iseppi, G., Mylonas, A., and Stavrou, V. (2018). Exiting the risk assessment maze: a meta-survey. ACM Computing Surveys (CSUR), 51(1), 11.
72. Hamburger, E., 2014. Facebook's new stats: 1.32 billion users, 30 percent only use it on their phone. The Verge, available at:http://www.theverge.com/2014/7/23/5930743/facebooks-new-stats-1-32-billion-users-per-month-30-percent-only-use-it-on-their-phones.[Accessed 20 May 2015].
73. Hayashi, E., Riva, O., Strauss, K., Brush, A., & Schechter, S., 2012 Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications, SOUPS, 2012.
74. Hoang, T., & Choi, D., 2014 Secure and privacy enhanced gait authentication on smart phone. The Scientific World Journal.
75. Hocking, C., Furnell, S., Clarke, N., and Reynolds, P., 2011 Authentication Aura - A distributed approach to user authentication. Journal of Information Assurance and Security.
76. Hong, F., Wei, M., You, S., Feng, Y., & Guo, Z., Waving authentication: your smartphone authenticate you on motion gesture In Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems. ACM, 2015, pp.263-266.

77. Hoofnagle, C. J., King, J., Li, S., & Turow, J., 2010, How different are young adults from older adults when it comes to information privacy attitudes and policies?

78. HSBC, 2016. Introducing Fast Balance, available at http://www.hsbc.co.uk/1/2/contact-and-support/ways-to-bank/fastbalance). [Accessed 20 May 2015]

79. Haes, S.D.; Grembergen, W.V. (2015). "Chapter 5: COBIT as a Framework for Enterprise Governance of IT". Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5 (2nd ed.). Springer. pp. 103–128. ISBN 9783319145471. Retrieved 24 June 2016.

80. IBG, 2010. How is biometric defined? International Biometric Group, available at: http://www.biometricgroup.com/reports/biometric_definition.html [Accessed 7 May 2015]

81. IDC, 2014. Smartphone OS Market Share, Q3 2014, [Online]. , available at: http://www.idc.com/prodserv/smartphone-os-market-share.jsp. [Accessed: 20 December 2014].

82. ISO 27000 (2016) : available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en

83. ITU.int, 2015. ICT Facts and Figures: The World in 2015, [online]. , available at: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf [Accessed 6 May2016]

84. Josang, A., Bradley, D., and Knapskog, S. J. (2004, January). Belief-based risk analysis. In Proceedings of the second workshop on Australasian

information security, Data Mining and Web Intelligence, and Software Internationalisation-Volume 32 (pp. 63-68). Australian Computer Society, Inc.

85. Jain, A., Nandakumar, K., & Ross, A. , 2005. Score normalization in multimodal biometric systems. Pattern recognition, 38(12), 2270-2285.
86. Jain, A., Flynn, P. & Ross, A., 2007. Handbook of Biometrics, New York, Springer
87. Jain, A., Prabhakar, S. & Pankanti, S., 2002. On the similarity of identical twin fingerprints, Pattern Recognition, vol.35, Issue: 11, pp.2653-2663
88. Jain, A., Ross, A. & Prabhakar, S., 2004. An introduction to biometric recognition, Circuits and Systems for Video Technology, IEEE Transactions on Circuits and Systems for Video Technology , vol.14, no.1, pp. 4-20,
89. Jakobsson , M., Shi ,E., & Chow, R., 2009 Implicit authentication for mobile devices, in 4th USENIX Workshop on Hot Topics in Security (HotSec 09), Montreal, Canada.
90. Juniper. (2018) available at :https://www.juniperresearch.com/document-library/white-papers/juniper-research-top-10-tech-trends-for-2018
91. Karatzouni, S. & Clarke, N., 2007 Keystroke Analysis for Thumb-based Keyboards on Mobile Devices. In Proc. IFIP International Information Security Conference (SEC), pp.253-263.
92. Karim, M. E., Balagani, K. S., Elliott, A., Irakiza, D., O'Neal, M., & Phoha, V. (2018). Active Authentication of Keyboard Users: Performance Evaluation on 736 Subjects. arXiv preprint arXiv:1804.08180.

93. Karnan, M., Akila M., & Krishnaraj, N.,2011 .Biometric Personal Authentication Using Keystroke Dynamics: A Review, Applied Soft Computing, vol. 11, no. 2, pp. 1565 –1573.

94. Kayacik, H., Just, M., Baillie, L., Aspinall, D., & Micallef, N., 2014 Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors, in Proceedings of the Mobile Security Technologies Workshop.

95. Keating, F., 2013. Got a smartphone? You probably check Facebook fourteen times a day. The Daily Mail. , available at http://www.dailymail.co.Uk/sciencetech/article-2300466/Smartphone-users-check-Facebook-14-timesday-admit-looking-movies.html. [Accessed 20th May 2015].

96. Kerr, D. 2014. Is Samsung's Galaxy S5 fingerprint scanner secure enough?', CNET website, 14th May 2014, ,available: http://www.cnet.com/uk/news/is-samsungs-galaxys5-fingerprint-scanner-secure-enough/ [Accessed 9 March 2015].

97. Ketabdar H., Roshandel, M., & Skripko, D., 2011. Towards implicit enhancement of security and user authentication in mobile devices based on movement and audio analysis. Interactions, pp.188-191.

98. Khan, H. & Hengartner, U., 2014. Towards application-centric implicit authentication on smartphones, in ACM HotMobile.

99. King, R., 2013, Google readies android 'KitKat' amid 1 billion device activations milestone, available at: http://www.zdnet.com/article/google-

readies-android-kitkat-amid-1-billion-device-activations-milestone/ [Accessed: 17 Nov 2015]

100. Koundinya, P., Theril, S., Feng, T., Prakash, V., Bao, J., & Shi, W. (2014). Multi-resolution touch panel with built-in fingerprint sensing support. In Design, Automation & Test in Europe Conference & Exhibition (DATE), 2014 (pp. 1-6). New Jersey: IEEE Conference Publications.

101. Külcü, Ö. and Henkoğlu, T., 2014. Privacy in social networks: An analysis of Facebook, International Journal of Information Management, 34(6), pp.761-769.

102. Kurkovsky, S., & Syta, E., 2010. Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. IEEE International Symposium on Technology and Society. IEEE, 441–449.

103. Katsini, C., Belk, M., Fidas, C., Avouris, N., & Samaras, G. (2016, November). Security and usability in knowledge-based user authentication: a review. In Proceedings of the 20th Pan-Hellenic Conference on Informatics (p. 63). ACM.

104. Khan, M. A., Din, I. U., Jadoon, S. U., Khan, M. K., Guizani, M., & Awan, K. A. (2019). G-RAT| A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices. IEEE Transactions on Consumer Electronics.

105. Ledermuller, T., & Clarke, N., 2011, Risk assessment for mobile devices". In Trust, Privacy and Security in Digital Business (pp. 210-221). Springer Berlin Heidelberg.

106. Lee, W., & Lee, R., 2015 Multi-sensor authentication to improve smartphone security. In Conference on Information Systems Security and Privacy.

107. Li, F., Clarke, N., Papadaki, M., & Dowland, P. (2011). Behaviour Profiling for Transparent Authentication for Mobile Devices. In the 10th European Conference on Information Warfare and Security (ECIW 2011) (pp. 307-314). Tallinn, Estonia.

108. Li, F., Clarke, N., Papadaki, M., & Dowland, P., 2011 Misuse detection for mobile devices using behaviour profiling, IJCWT, vol. 1, no. 1, pp.41-53.

109. Li, F., Clarke, N., Papadaki, M., & Dowland, P., 2014 Active authentication for mobile devices utilising behaviour profiling. International journal of information security, 13(3), pp.229-244.

110. Lamiche, I., Bin, G., Jing, Y., Yu, Z., and Hadid, A. (2018). A continuous smartphone authentication method based on gait patterns and keystroke dynamics. Journal of Ambient Intelligence and Humanized Computing, 1-14.

111. Li, L., Zhao, X., and Xue, G., 2013 Unobservable re-authentication for smartphones. In NDSS.

112. Lin, C., Liang, D., Chang, C., and Yang, C., 2012 A new non-intrusive authentication method based on the orientation sensor for smartphone users, in IEEE Sixth International Conference on Software Security and Reliability (SERE), pp.245-252.

113. Maglogiannis, I., Zafiropoulos, E., Platis, A., and Lambrinoudakis, C. (2006). Risk analysis of a patient monitoring system using Bayesian Network modeling. Journal of Biomedical Informatics, 39(6), 637-647.

114. Maglogiannis, I., & Zafiropoulos, E. (2006, August). Modeling risk in distributed healthcare information systems. In 2006 International Conference of the IEEE Engineering in Medicine and Biology Society (pp. 5447-5450). IEEE.

115. MacAfee, 2015. Threats Predictions [online]. , available at: http://www.mcafee.com/es/resources/misc/infographicthreats- predictions-2015.pdf [Accessed 24 September 2015].

116. Maiorana, E., Campisi, P., González-Carballo, N., & Neri, A., 2011 Keystroke dynamics authentication for mobile phones. In Proceedings of the Symposium on Applied Computing. ACM, pp.21-26.

117. Manavati S., Thieme M., & Nanavati, R., 2002. Biometrics: Identity Verification in a Net-worked World. John Wiley & Sons, Inc., 320.

118. Markets and Markets, 2011. Global Biometrics Technology Market (2010-2015) – Market Forecast by Products, End-User Application and Geography. , available at: http://www.marketsandmarkets.com/Market-Reports/biometric-market-278.html [Accessed 8 April 2015]

119. McAfee, 2010. McAfee Threats Report: Fourth Quarter 2010, available at: https://secure.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2010.pdf, [Accessed 5 April 2016]

120. Meitiv, A., 2010. Are Android unlock patterns as secure as numeric PINs?' Mathematics, 14th April 2010, available at: http://playingwithmodels.wordpress.com/ 2010/04/14/andorid_unlock_patterns/ [Accessed 5 April 2016]

121. Meng, W., Wong, D., Furnell, S., & Zhou, J., 2015 Surveying the development of biometric user authentication on mobile phones, IEEE Communications Surveys & Tutorials.

122. Miles, G., 2015. 8 Mobile Marketing Stats to Help You Plan For 2016, 2015, available at: http://www.socialmediatoday.com/marketing/8-mobile-marketing-stats-help-you-plan-2016 [Accessed 9th December 2015]

123. Mock, K., Hoanca, B., Weaver, J., & Milton, M. (2012). Real-time continuous iris recognition for authentication using an eye tracker. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 1007-1009). ACM.

124. Muaaz, M. & Mayrhofer, R. 2014 Orientation independent cell phone based gait authentication. In Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia. ACM, pp.161-164.

125. Muaaz, M., & Mayrhofer, R., 2013 . An analysis of different approaches to gait recognition using cell phone based accelerometers. In Proceedings of International Conference on Advances in Mobile Computing and Multimedia. ACM, p.293

126. Mylonas, A., Theoharidou, M., & Gritzalis, D., 2013. Assessing privacy risks in android: A user-centric approach. In Risk Assessment and Risk-Driven Testing (pp. 21-37). Springer International Publishing.

127. Mahfouz, A., Mahmoud, T. M., & Eldin, A. S.A survey on behavioral biometric authentication on smartphones. Journal of Information Security and Applications, 37, 28-37. 2017.

128. Nickel, C., Wirt, T., and Busch, C., 2012 Authentication of smartphone users based on the way they walk using k-NN algorithm. In Intelligent Information Hiding and Multimedia Signal Processing.

129. NIST S 800-30. 2012. Guide for conducting risk assessments. 800–830. Revision 1.

130. Nielsen, 2014, Smartphones: So Many Apps, So Much Time'; http://www.nielsen.com/us/en/insights/news/2014/smartphones-so-many-apps--so-much-time.html (9 November 2015).

131. O' Boyle, B., 2014. How does the Samsung Galaxy S5 fingerprint scanner work?', Pocket-lint website, ,,available at : http://www.pocket-lint.com/news/127605-how-does-the-samsung-galaxy-s5-fingerprint-scanner-work [Accessed: 17 Nov 2014]

132. O'Gorman, L., 2003. Comparing Passwords, Tokens, and Biometrics for User Authentication, Proceedings of the IEEE, vol. 91, no. 12, pp. 2019-2040

133. Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. IEEE Signal Processing Magazine, 33(4), 49-61.

134. Raghavendra, R., Busch, C., & Yang, B. (2013, September). Scaling-robust fingerprint verification with smartphone camera in real-life scenarios. In Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on (pp. 1-8). IEEE.

135. Raja, K., Raghavendra, R., Stokkenes, M., & Busch, C., 2015. Multi-modal authentication system for smartphones using face, iris and periocular. In Biometrics (ICB); 2015 International Conference on, pp.143–150.

136. Riva, O., Qin, C., Strauss, K., & Lymberopoulos, D., 2012. Progressive authentication: Deciding when to authenticate on mobile phones, in Proceedings of the 21st USENIX Conference on Security Symposium, ser. Security'12. Berkeley, CA, USA: USENIX Association.

137. Rodwell, M., Furnell, S. & Reynolds, L., 2007. A non-intrusive biometric authentication mechanism utilising physiological characteristics of human head, Computer & Security, vol.26, no.7, pp.468-478

138. Ross, A. & Jain, A., 2004. Multimodal Biometrics: An Overview', Proceedings of 12th European Signal Processing Conference (EUSIPCO), pp. 1221-1224.

139. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal, 40(3), 614-634.

140. Ross, A. A., & Govindarajan, R. (2005, March). Feature level fusion of hand and face biometrics. In Biometric Technology for Human Identification II (Vol. 5779, pp. 196-205). International Society for Optics and Photonics.

141. Ross, A., 2011. Advances in Ear Biometrics. Presentation at West Virginia University, 1-34.

142. Saevanee, H., 2014. Continuous User Authentication Using Multi-Modal Biometrics, PhD

143. Saevanee, H., Clarke, N., & Furnell, S., 2012, Multi-modal behavioural biometric authentication for mobile devices, In Proc. IFIP Information Security and Privacy Conference (SEC), pp.465-474. MSP), 2012 Eighth International Conference on. IEEE, pp.16-20.

144. Saevanee, H., Clarke, N., Furnell, S., & Biscione, 2014 Text-based active authentication for mobile devices. In ICT Systems Security and Privacy Protection. Berlin Heidelberg: Springer, pp.99-112.

145. Saevanee, H., Clarke, N., Furnell, S., & Biscione, V. (2015). Continuous user authentication using multi-modal biometrics. Computers & Security, 53, 234-246.

146. Samsung, 2018 http://www.samsung.com/sa_en/smartphones/galaxy-s9/

147. Shahzad, M., Liu, A., & Samuel, A. 2013. Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you cannot do it. In Proc. of the 19th Annual Int. Conf. on Mobile Computing and Networking, pp.39-50.

148. Shen, C., Zhang, Y. , Cai, Z., Yu, T., & Guan, X., 2015, Touch-interaction behaviour for continuous user authentication on smartphones. In Biometrics (ICB), International Conference on. IEEE, pp.157-162.

149. Shi, E., Niu, Y., Jakobsson, M., & Chow, R., 2011b, Implicit authentication through learning user behaviour. In Information Security. Berlin Heidelberg: Springer, 2011, pp.99-113.

150. Sepczuk, M., and Kotulski, Z. (2018). A new risk-based authentication management model oriented on user's experience. Computers & Security, 73, 17-33.

151. Shen, C., Li, Y., Chen, Y., Guan, X., and Maxion, R. A. (2018). Performance analysis of multi-motion sensor behavior for active smartphone authentication. IEEE Transactions on Information Forensics and Security, 13(1), 48-62.

152. Shi, W., Yang, J., Jiang, Y., Yang, F., & Xiong, Y., 2011 SenGuard: passive user identification on smartphones using multiple sensors. 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Shanghai, China. Pp.141- 148.

153. Shoniregun, C., 2006 .Impacts and Risk Assessment of Technology for Internet Security: Enabled Information Small-Medium Enterprises (TEISMES) (Vol. 17). Springer Science & Business Media.

154. Siciliano, R., 2013, more than 30% of people don't password protect their mobile devices, available at: https://blogs.mcafee.com/consumer/unprotected-mobile-devices/ [Accessed 7 March 2016].

155. Sitova, Z., Sedenka, J., Yang Q., Peng G., Zhou G., Gasti P., & Balagani K., 2015 HMOG: a new biometric modality for continuous authentication of smartphone users, arXiv preprint arXiv.

156. Sun, Yan, Hayreddin Ceker, and Shambhu Upadhyaya. (2016) "Shared keystroke dataset for continuous authentication." IEEE International Workshop on information Forensics and Security (WIFS): 1-6.

157. Smart Insights, 2015. Statistics on consumer mobile usage and adoption to inform your mobile marketing strategy mobile site design and app development, available at: http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/[Accessed 3th February 2016]

158. Spaccapetra, S., Al-Jadir, L., Yu, S., 2005, somebody, sometime, somewhere, something Proceedings of the 2005 workshop on Ubiquitous Data Management. Tokyo, Japan, pp. 6-16

159. Statista, 2015. Number of apps, available in leading app stores as of July 2015, [online]. , available at: http://www.statista.com/statistics/276623/number-ofapps-, available-in-leading-app-stores/ [Accessed 14th November 2015].

160. Statista, 2016 b. worldwide mobile app revenues in 2015, 2015 and 2020 (in billion U.S. dollars), available at: http://www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/ [Accessed 21th November 2015]

161. Statista, 2016 c. Number of, available applications in the Google Play Store from December 2009 to February 2016 http://www.statista.com/statistics/266210/number-of-,available-applications-in-the-google-play-store/ [Accessed 21th November 2015]

162. Statista, 2016 d. Number of mobile app users in the United Kingdom from third quarter 2013 to second quarter 2016 ,available at: http://www.statista.com/statistics/277672/forecast-of-mobile-app-users-in-the-united-kingdom-uk/ [Accessed 14th March 2016].

163. Statista, 2016 e. Android and iOS are the Last Two Standing, available at: https://www.statista.com/chart/4431/smartphone-operating-system-market-share/ [Accessed 21th November 2015]

164. Statista, 2016. Forecast: smartphone users in the United Kingdom (UK) 2011-2018,available

at:http://www.statista.com/statistics/270821/smartphone-user-in-the-united-kingdom-uk/[Accessed 4th September 2015]

165. Statista, 2018: Number of smartphone users worldwide from 2014 to 2020 (in billions) available at https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

166. Stutzman, F., Grossy, R., & Acquisti, A., 2012. Silent listeners: The evolution of privacy and disclosure on Facebook. Journal of Privacy and Condentiality, 4(2), 7–41.

167. Tam, K., Khan, S.J., Fattori, A. and Cavallaro, L., 2015. CopperDroid: Automatic Reconstruction of Android Malware Behaviors, InNDSS.

168. Tang, Y., Hidenori, N., & Urano, Y., 2010 User authentication on smart phones using a data mining method, International Conference on Information Society IEEE, pp.173-178.

169. Tanvi P, Sonal G, Kumar SM. 2011. Token based authentication using mobile phone. In: Proc. international conference on communication systems & network technologies (CSNT).

170. Tanviruzzaman, M., & Ahamed, S., 2014. Your phone knows you: almost transparent authentication for smartphones. IEEE 38th Annual Computer Software and Applications Conference. IEEE, pp.374–383.

171. Tao, Q., & Veldhuis, R. (2010). Biometric authentication system on mobile personal devices. IEEE Transactions on Instrumentation and Measurement, 59(4), 763-773.

172. Theoharidou, M., Mylonas, A. and Gritzalis, D., 2012. A risk assessment method for smartphones. In Information security and privacy research (pp. 443-456). Springer Berlin Heidelberg.

173. Traore I., & Ahmed, A., 2012 Introduction to Continuous Authentication: In Continuous Authentication Using Biometrics. IGI Global, 2012, pp.1-22.

174. Tresadern, P., Cootes, T., Poh, N., Matejka, P., Hadid, A., Levy, C., & Marcel S., 2013 Mobile Biometrics (MoBio): joint face and voice verification for a mobile platform. In IEEE pervasive computing, pp.79-87.

175. Trojahn, M., & Ortmeier, F., 2013. Toward mobile authentication with keystroke dynamics on mobile phones and tablets. In Advanced Information Networking and Applications Workshops (WAINA), 27th International Conference on. IEEE, pp.697-702.

176. Verizon Business Security Solutions, 2012. Data Breach Investigations Report, available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf, [Accessed 14 March 2015]

177. Wang, H., Lymberopoulos, D. & Liu, J., 2015 Sensor-based user authentication, In Wireless Sensor Networks. Springer International Publishing, pp.168-185.

178. Watanabe, Y., 2015. Toward application of immunity-based model to gait recognition using smart phone sensors: A study of various walking States. Procedia Computer Science, 60, pp.1856-1864.

179. We are social report, 2016. , available at: http://wearesocial.com/uk/special-reports/digital-in-2016 [Accessed 7 October 2015]

180. Woo, R. H., Park, A., & Hazen, T. J. (2006). The MIT Mobile Device Speaker Verification Corpus: Data Collection and Preliminary Experiments. In IEEE Odyssey 2006: The Speaker and Language Recognition Workshop, 2006. (Vol. 0, pp. 1-6). IEEE.

181. Wood, H., 1977. The Use of Passwords for Controlling Access to Remote Computer Systems and Services', Proceedings of American Federation of Information Processing Societies: 1977 National Computer Conference (AFIPS 77), Dallas, Texas, USA, 13-16 June 1977, pp. 27-33

182. Wangen, G., Hallstensen, C., and Snekkenes, E. (2017). A framework for estimating information security risk assessment method completeness. International Journal of Information Security, 1-19.

183. Woodward, J., Orlans, N., |&Higgins, P., 2003. Identity Assurance in the Information Age. McGraw-Hill/Osborne, Berkeley, California.

184. Xu, H., Zhou, Y., & Lyu, M.R., 2014. Towards continuous and passive authentication via touch biometrics: an experimental study on smartphones, In Proc. SOUPS, pp.187-198.

185. Xiaofeng, L., Shengfei, Z., & Shengwei, Y. (2019). Continuous authentication by free-text keystroke based on CNN plus RNN. Procedia Computer Science, 147, 314-318.

186. Yang, L., Guo Y., Ding X., Han J., Liu Y., C. Wang, & C. Hu, 2015 Unlocking smart phone through hand waving biometrics. In Mobile Computing. IEEE, pp.1044-1055.

187. Yousefpor, M., Bussat, J., Lyon B., Gozzini, G., Hotelling, S., & Setlak D., 2014 Fingerprint sensor in an electronic device, U.S. Patent Application 14/451,076.

188. Yang, Y., Guo, B., Wang, Z., Li, M., Yu, Z., & Zhou, X. (2019). BehaveSense: Continuous authentication for security-sensitive mobile apps using behavioral biometrics. Ad Hoc Networks, 84, 9-18.

189. Zahid, S., Shahzad, M., Khayam, A., & Farooq, M., 2009, Keystroke-based user identification on smart phones. In Recent Advances in Intrusion Detection. Berlin Heidelberg: Springer, pp.224-243.

190. Zheng, N., Bai, K., Huang, H., & Wang, H., 2014 You are how you touch: User verification on smartphones via tapping behaviours, WM-CS-2012- 06, Tech. Rep.

191. Zhao, J., Li, Y., Wu, J., & Liao, Q. (2018, January). Predict what app to use next time only consider time and latest used app context. In Proceedings of the 2018 2nd International Conference on Management Engineering, Software Engineering and Service Sciences (pp. 163-166). ACM.

192. Zhou, Y. & Jiang, X., 2012. Dissecting android malware: Characterization and evolution, in Proc. of the IEEE Symposium on Security and Privacy.

193. Zhu, J., Wu, P., Wang, X., & Zhang, J., 2013 SenSec: mobile security through passive sensing. In Proc. of the 13th Int. Conf. on Computing, Networking and Communications.

194. Zhu, H., Hu, J., Chang, S., Lu, L., 2017. ShakeIn: secure user authentication of smartphones with single-handed shakes. IEEE Trans. Mobile Comput. 16, 2901-2912.

Appendices

Appendix A – Ethical Approval

RESEARCH WITH PLYMOUTH UNIVERSITY

20 January 2017

CONFIDENTIAL
Saud Alotaibi
School of Computing, Electronics and Mathematics

Dear Saud

Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

A Transparent Intra-Process Security Framework for Mobile Applications

I am pleased to inform you that this has been approved.

Kind regards

Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Prof Steven Furnell
Prof Nathan Clarke

Faculty of Science and Engineering
Plymouth University
Drake Circus
PL4 8AA

T +44 (0) 1752 584 584
F +44 (0) 1752 584 540
W www.plymouth.ac.uk

Mrs Jayne Brenen
Head of Faculty Operations

Fri 20/01/2017 16:13

Paula Simson on behalf of Science and Engineering Human Ethics

RE: ethical approve of my research project

To Saud Alotaibi

Cc Steven Furnell; Nathan Clarke

Follow up. Start by 21 January 2017. Due by 21 January 2017.
You forwarded this message on 10/08/2017 10:46.

Message | Approval Letter (2).pdf (29 KB)

Dear Saud

Thank you very much for clarifying this. Please find attached an updated approval letter.

Regards
Paula

Appendix B - Consent Form

SAMPLE SELF-CONSENT FORM

PLYMOUTH UNIVERSITY

FACULTY OF SCIENCE AND ENGINEERING

Human Ethics Committee Sample Consent Form

CONSENT TO PARICIPATE IN RESEARCH PROJECT / PRACTICAL STUDY

Name of Principal Investigator

Saud Alotaibi

Title of Research
A Transparent Intra-Process Security Framework For Mobile Applications

Brief statement of purpose of work

Mobile phones are used to perform activities such as sending emails, transferring money via mobile Internet banking, shopping online and making calls. Additionally, after the point-of-entry authentication stage at the beginning of a session, using modalities such as a PIN or password, the user of the device can perform almost all tasks with different risk levels without having to periodically re-authenticate to re-validate the user's identity. As a result, our uses of mobile devices arguably require something stronger than current methods provide. This study seeks to suggest a method to be applied continuously and transparently without obstructing the users' activities to authenticate legitimate users, maintained beyond point-of-entry, without the explicit involvement of the user.

Therefore, this experiment seeks to capture and collect metadata of a log file only of some available mobile applications such as timestamp for each action within application from a real and live usage, in order to evaluate the appropriateness and effectiveness of utilising them for such authentication mechanism. Furthermore, there is no application will be installed on users mobile phones and thereby this solution is being able to protect user privacy.

As a participant, the principal investigator will connect your device to his computer to extract logs file information such as timestamp, application name, and process name after taking a backup from your device after 1 month of normal usage. The backup file will be removed at the end of the experiment period. During extraction the data, you will be invited to identify the level of impact consequence (Low, Medium, or High) for some actions within application. Upon completing the experiment duration, the log files will be generated in a datasheet format files on research devices. The data will be shown to you – once you are happy with them, the files will be taken by the principal investigator and will be anonymous and stored

in a secure location within the Centre for Security, Communications and Network Research (CSCAN) at Plymouth University.

At all stages of the study, confidentiality of the collected data and subsequent analysis will be maintained. At no time, will any identifying information about the participants be used in any publication or research output.

You have the right to withdraw at any stage upon until the completion of the data collection process. Should you wish to withdraw from the study, please contact Saud Alotaibi.

For information regarding the study, please contact: Saud Alotaibi - saud.alotaibi@plymouth.ac.uk

For any questions concerning the ethical status of this study, please contact the secretary of the Human Ethics Committee – paula.simson@plymouth.ac.uk

---

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far as possible, to avoid any risks, and that safety and health risks will have been separately assessed by appropriate authorities (e.g. under COSHH regulations)

Under these circumstances, I agree to participate in the research.

Name: .....

Signature: ..... Date: .....

Appendix C – Information Sheet (Data Collection)

SAMPLE INFORMATION SHEET FOR ADULT

PLYMOUTH UNIVERSITY

FACULTY OF SCIENCE AND ENGINEERING

RESEARCH INFORMATION SHEET

Name of Principal Investigator
Saud Alotaibi

Title of Research
A Transparent Intra-Process Security Framework For Mobile Applications

Aim of research

This experiment is part of a PhD research focuses on security and usability in the field of user authentication for mobile device security. Thus, this experiment is being conducted to explore the feasibility of building a transparent and continuous biometric-based authentication system that would provide a more secure, and user-friendly for mobile applications. Therefore, this experiment seeks to capture and collect metadata of a log file only of some available mobile applications such as timestamp for each action within application from a real and live usage.

Description of procedure

A log file only of some available mobile applications will be captured. Participants will not need to do anything but merely using their device(s) in their normal fashion. The data will be collected over a one-month period of normal usage. Furthermore, there is no application will be installed on users mobile phones and thereby this solution is being able to protect user privacy.

Description of risks

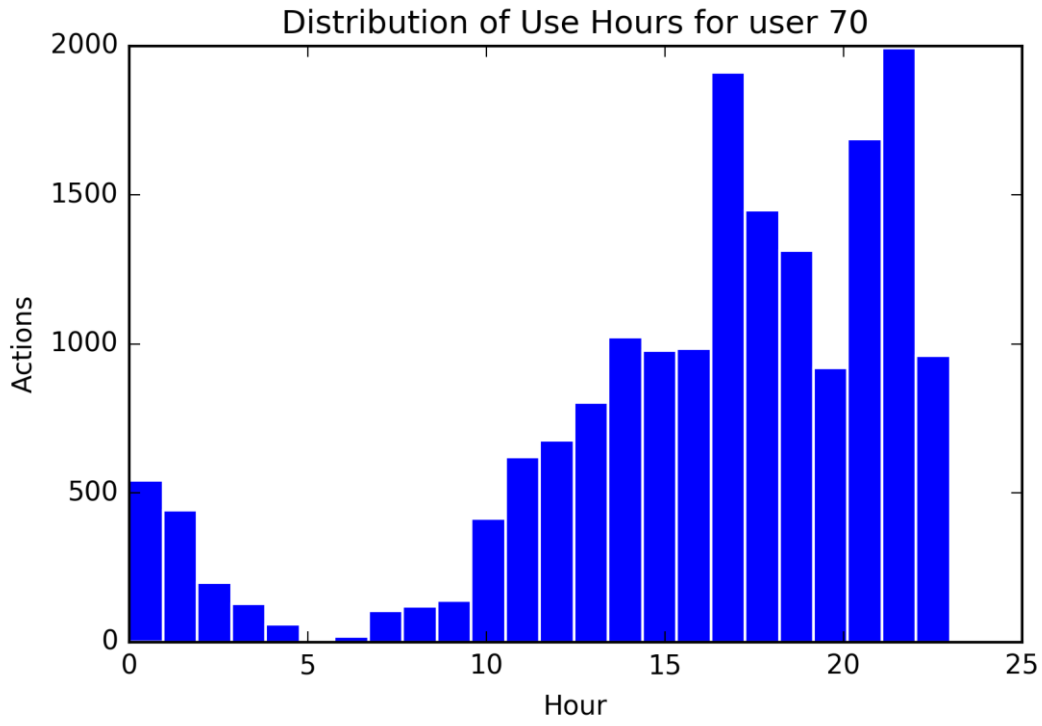
At no stage will any personally identifiable information be seen by any individual neither the researchers nor on any publication. The captured data will be stored after being converted to measurement features. All of the information will be treated confidentially and data will be anonymous during the collection, storage and publication of research material.

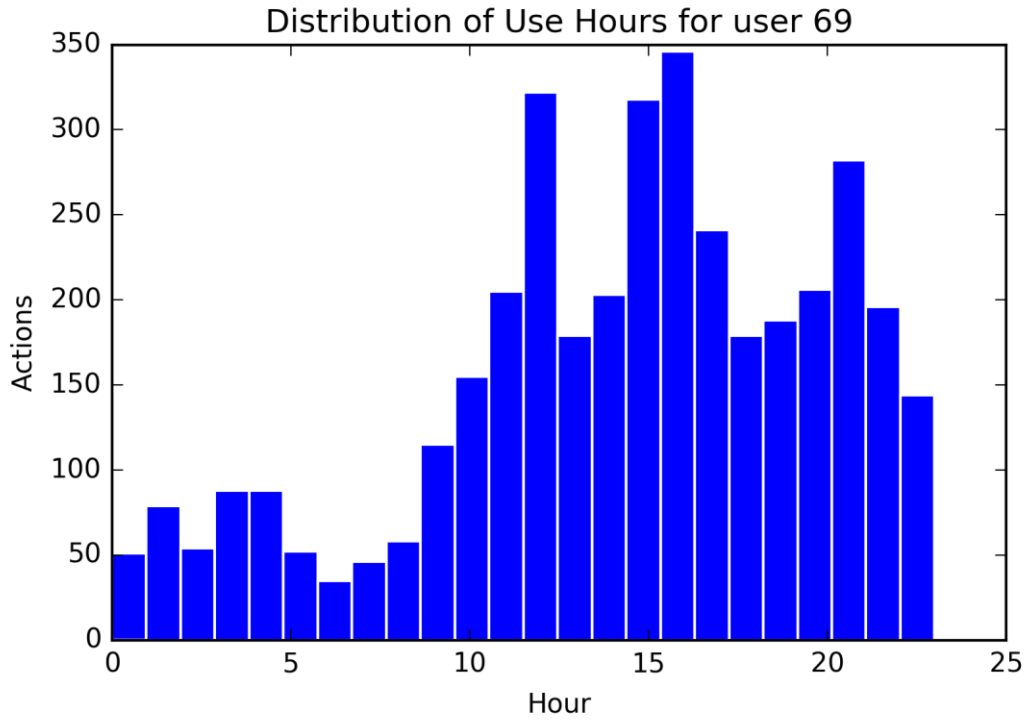
Benefits of proposed research
The ultimate aim of this research project is to build upon existing research on transparent authentication. An authentication system built upon this would provide a more secure, and user-friendly for mobile applications.

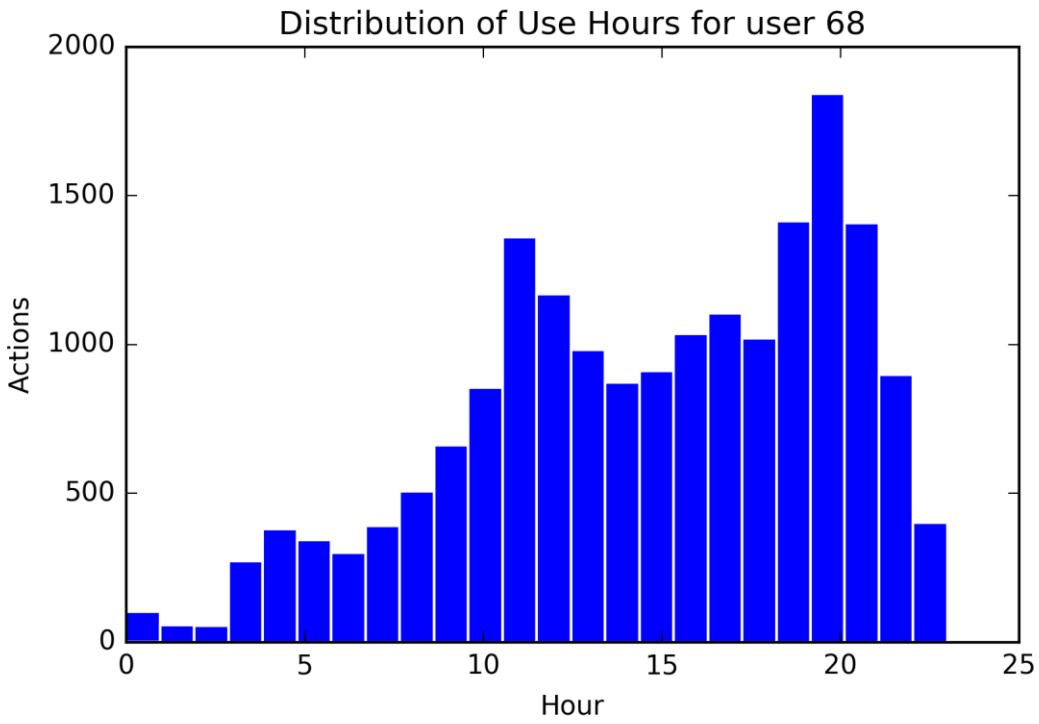
Right to withdraw

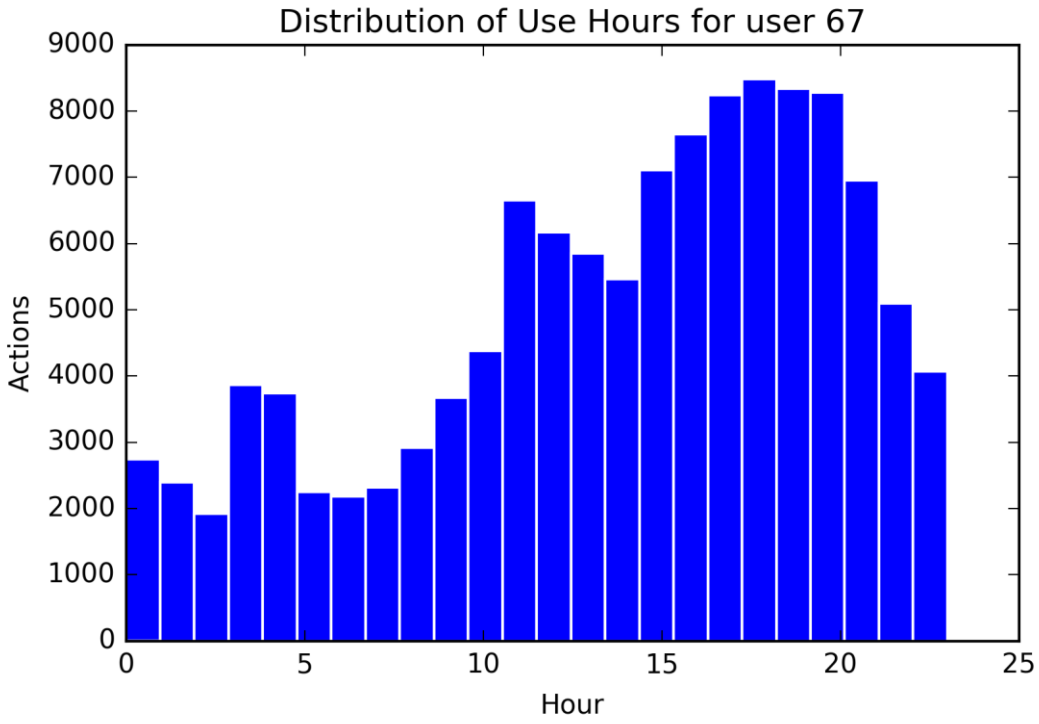
You have the right to withdraw at any stage without giving a reason. Your data will be removed and securely deleted.

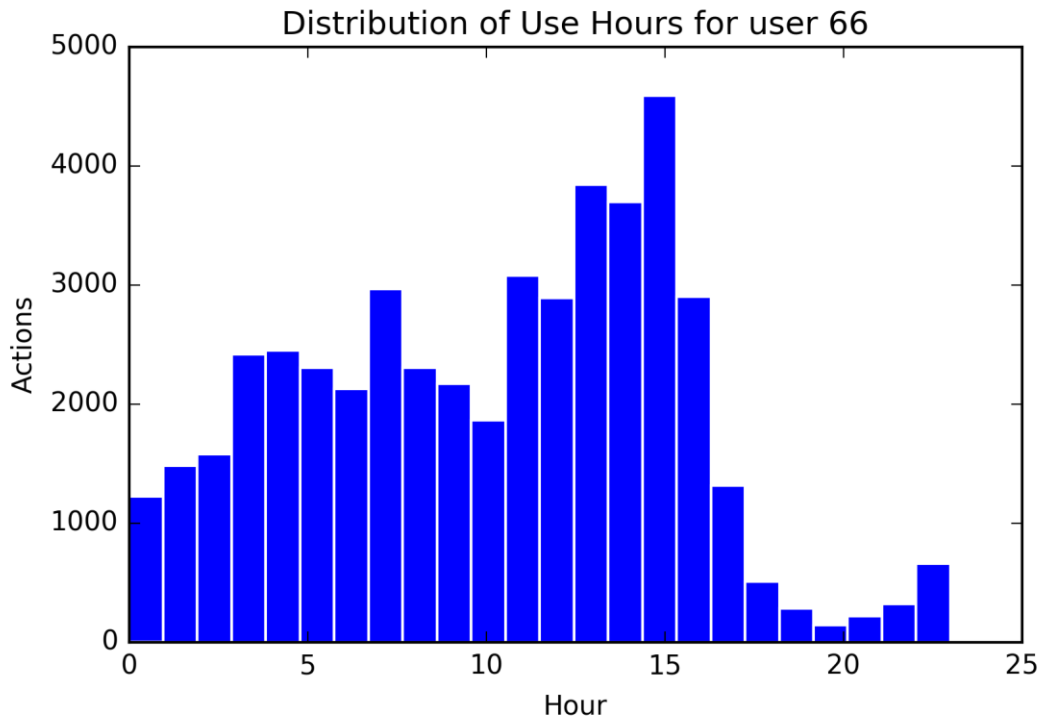
Appendix D – Distribution of Participants' User Hours

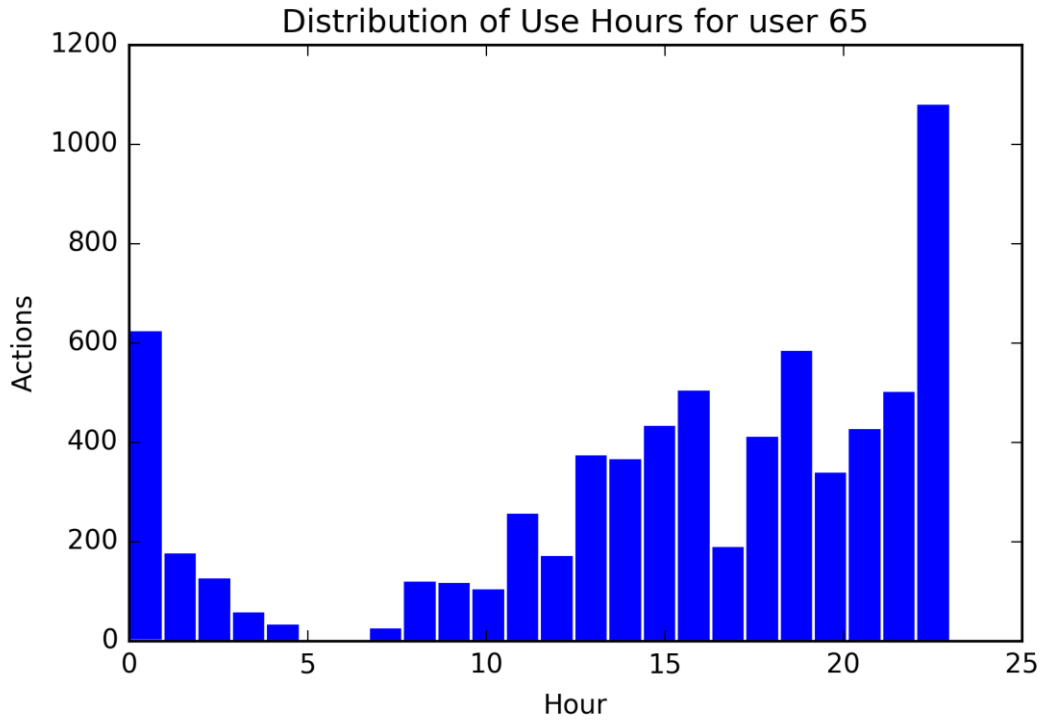


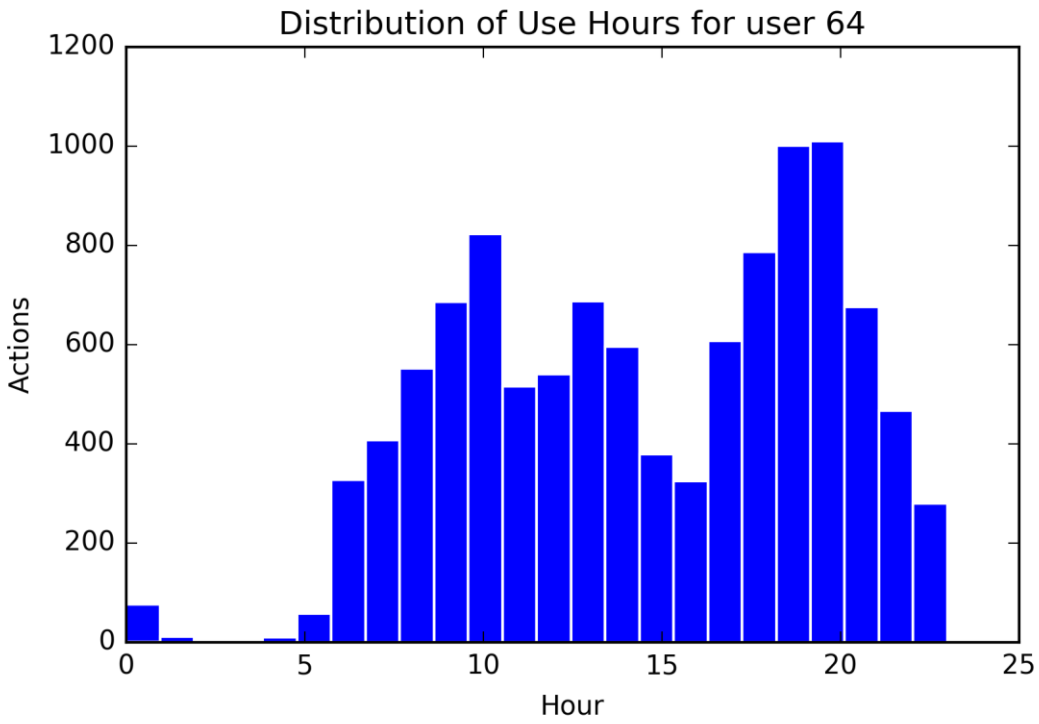


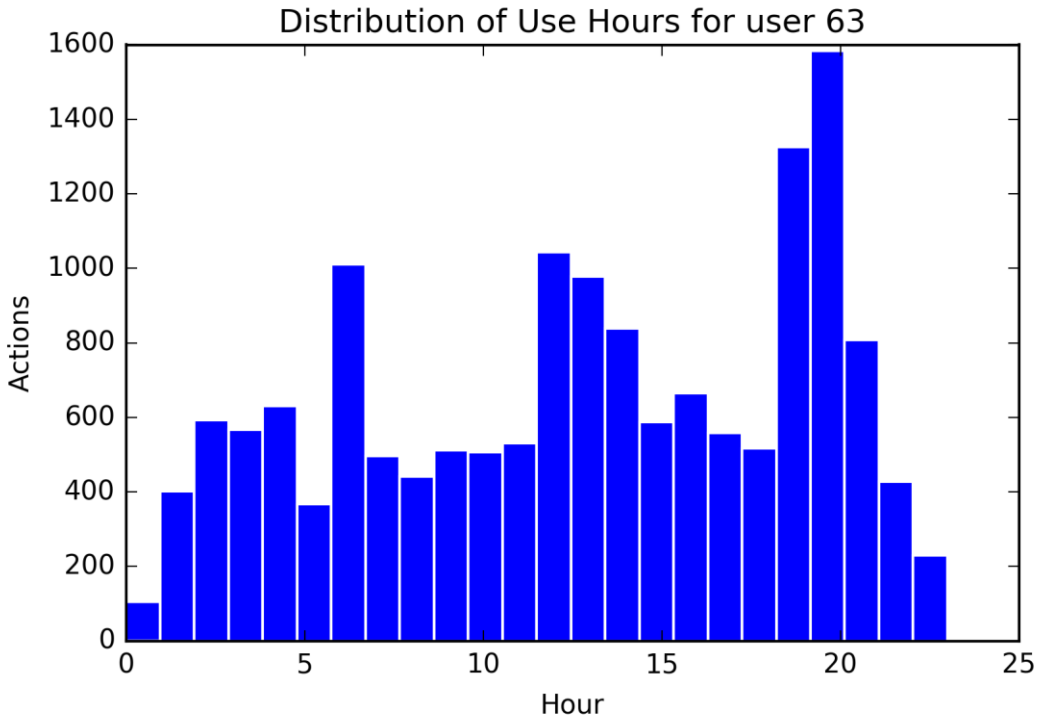

Distribution of Use Hours for user 68
Actions
Hour
0
500
1000
1500
2000
0
5
10
15
20
25

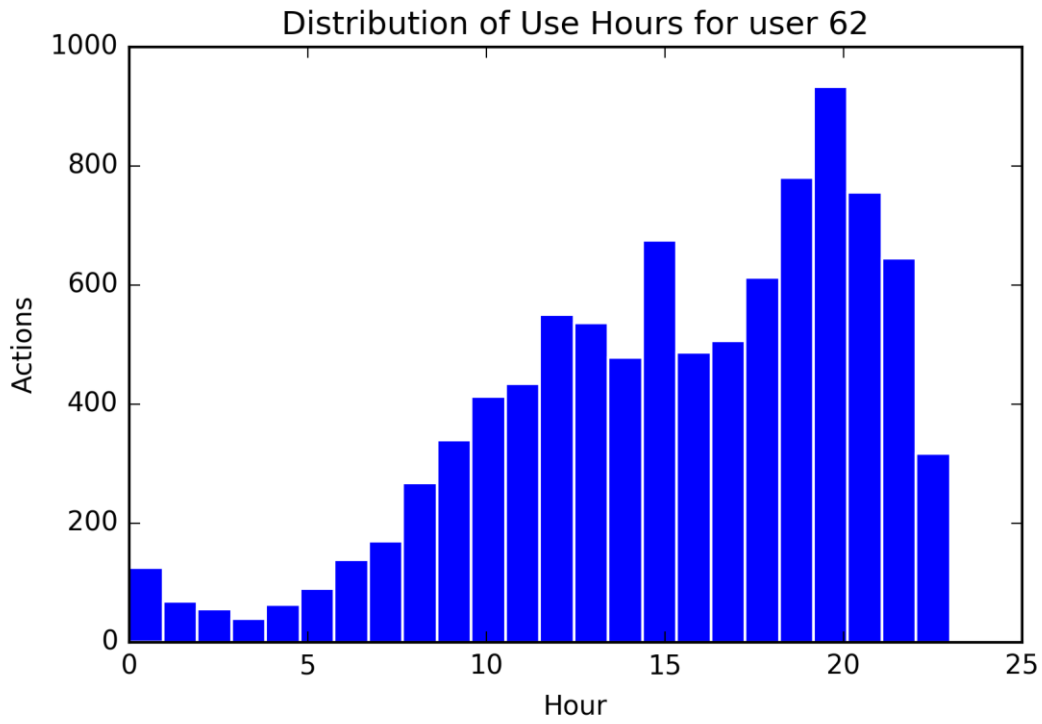

Distribution of Use Hours for user 67
Actions
Hour
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
0
5
10
15
20
25

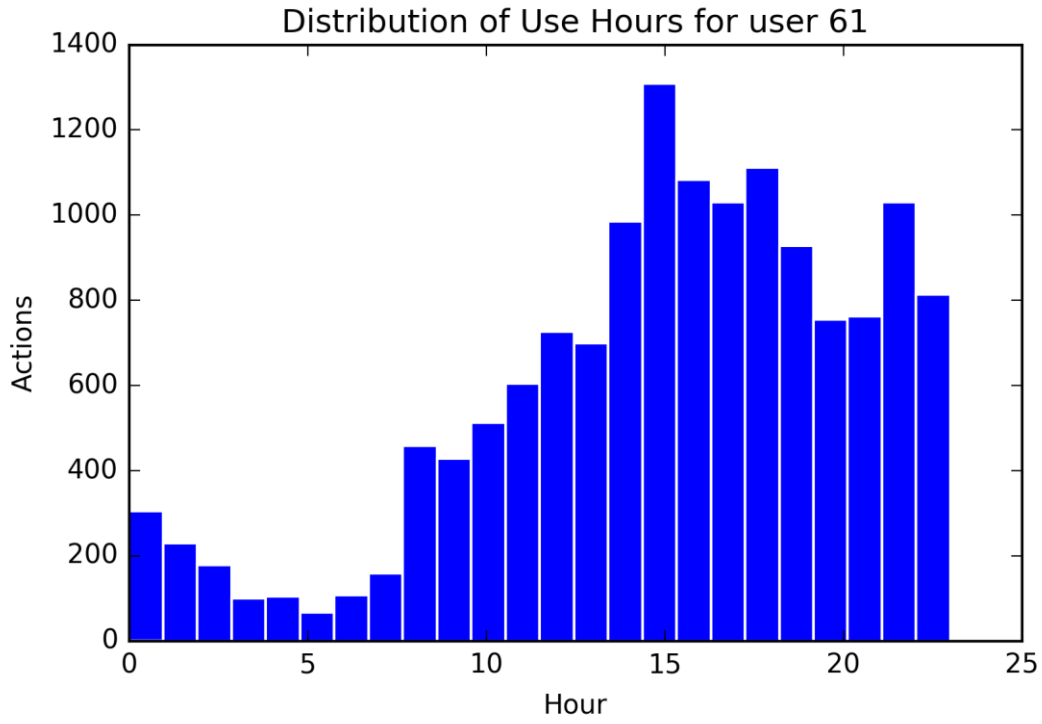

Distribution of Use Hours for user 66
Actions
Hour
0
1000
2000
3000
4000
5000
0
5
10
15
20
25

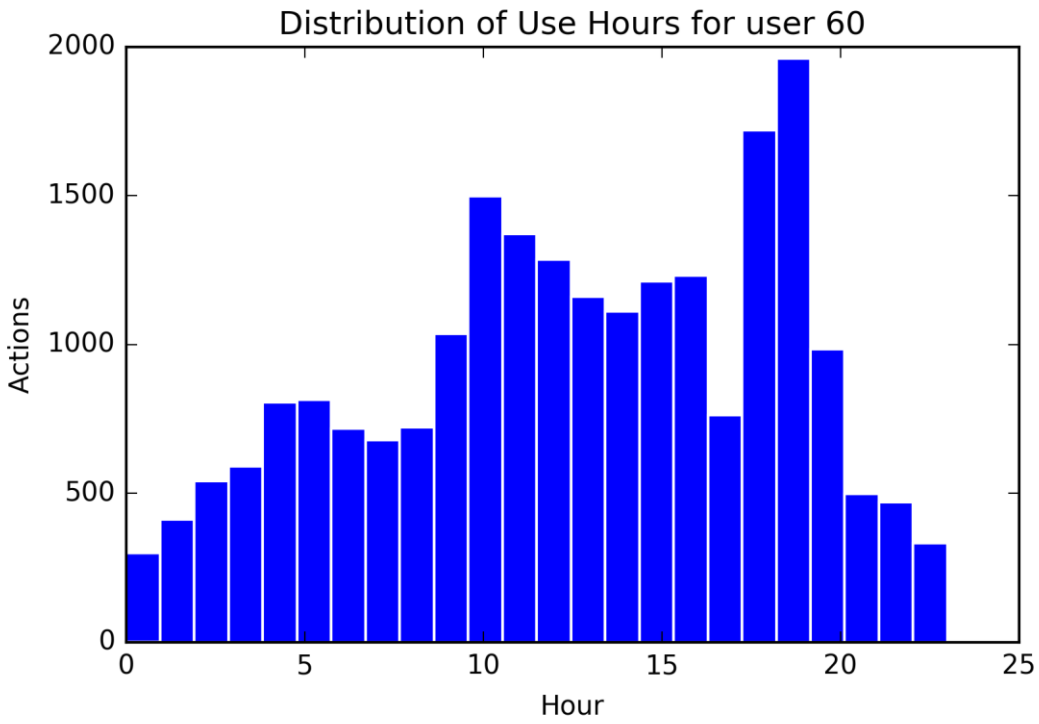

Distribution of Use Hours for user 65
Actions
Hour
0
200
400
600
800
1000
1200
0
5
10
15
20
25

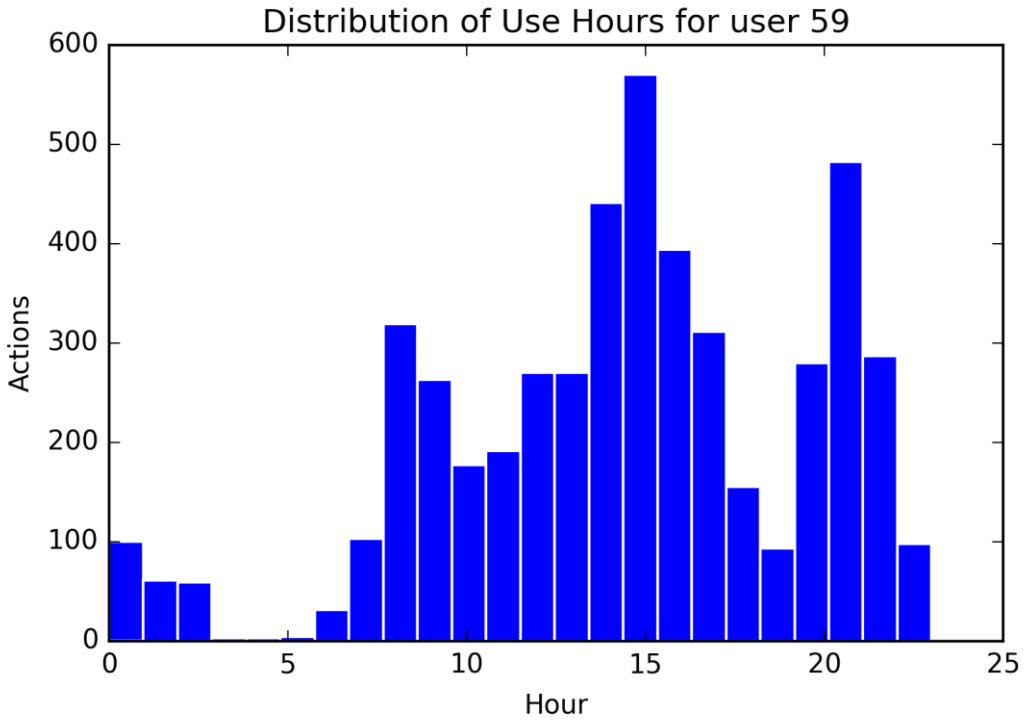

Distribution of Use Hours for user 64
Actions
Hour
0
200
400
600
800
1000
1200
0
5
10
15
20
25

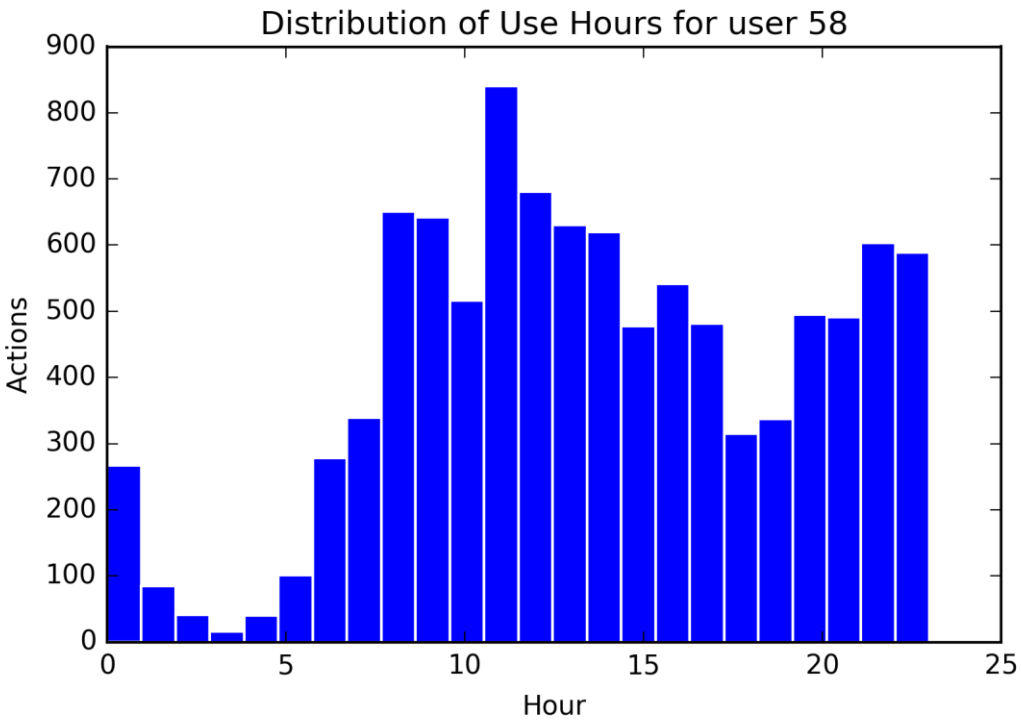

Distribution of Use Hours for user 63
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25

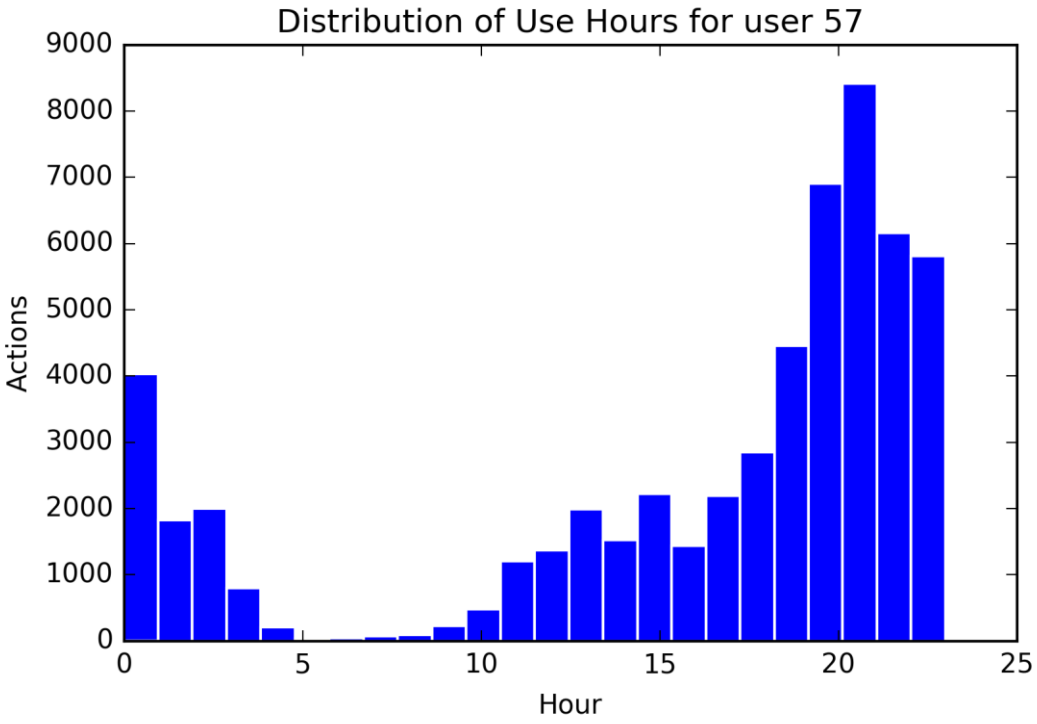

Distribution of Use Hours for user 62
Actions
Hour
0
200
400
600
800
1000
0
5
10
15
20
25

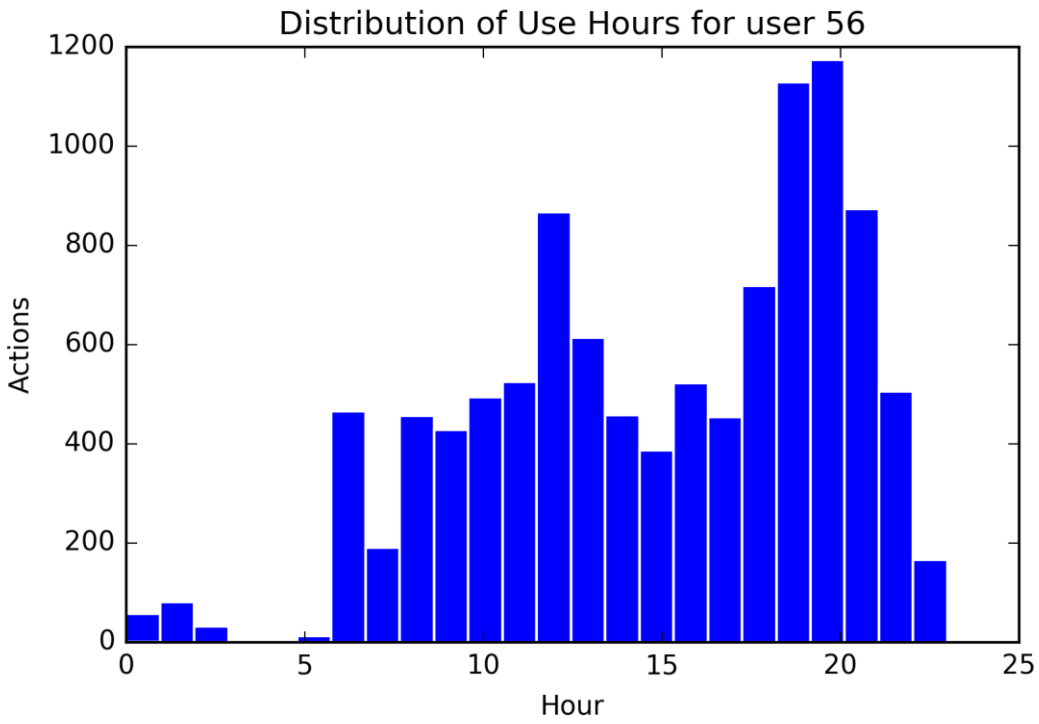

Distribution of Use Hours for user 61
Actions
Hour
0
200
400
600
800
1000
1200
1400
0
5
10
15
20
25

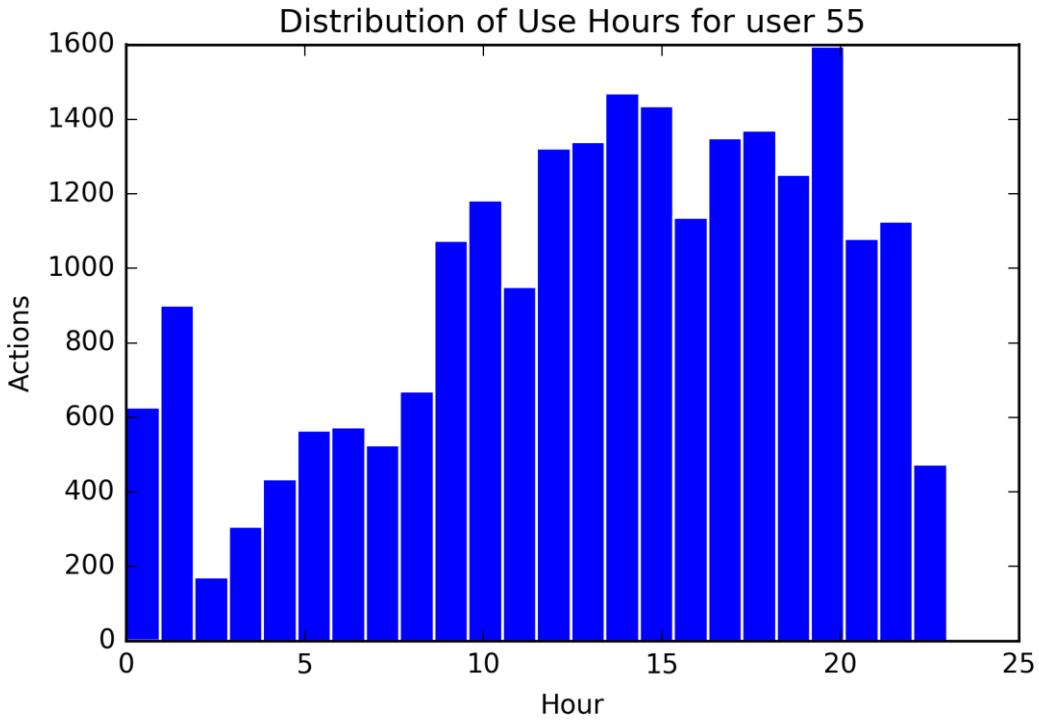

Distribution of Use Hours for user 60
Actions
Hour
0
500
1000
1500
2000
0
5
10
15
20
25

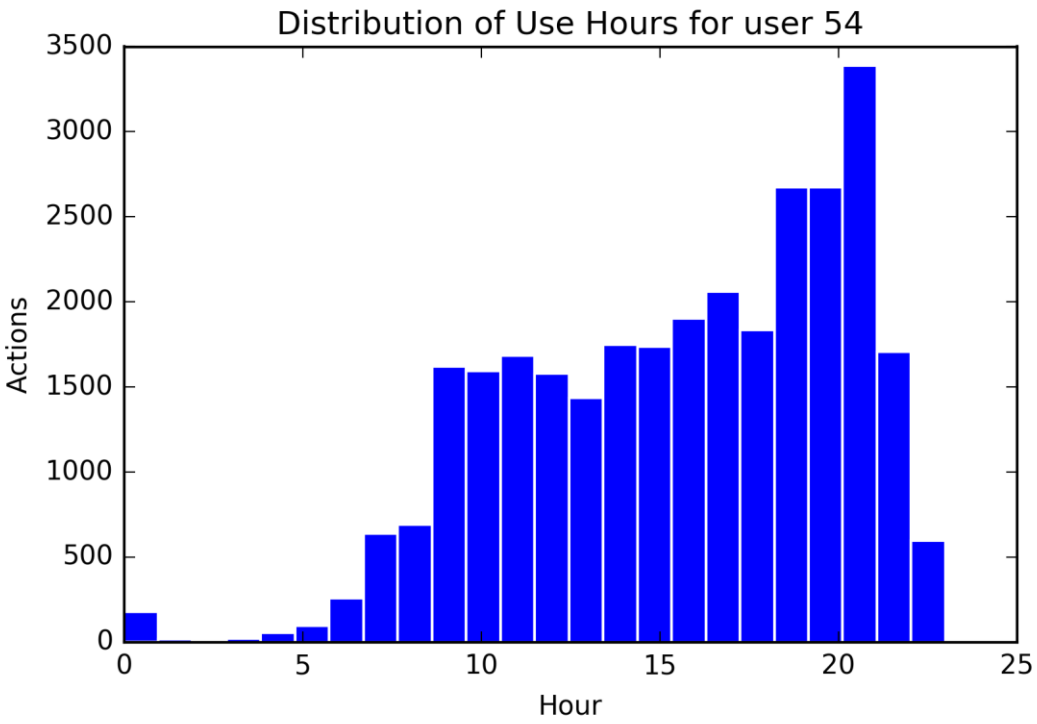

Distribution of Use Hours for user 59
Actions
Hour
0
100
200
300
400
500
600
0
5
10
15
20
25

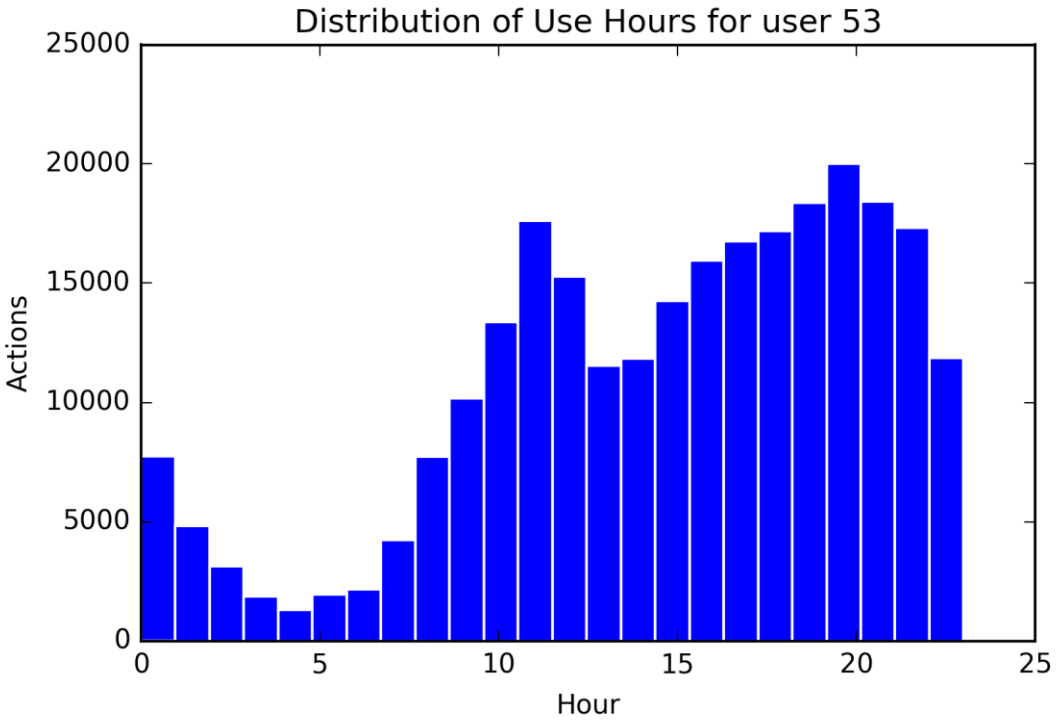

Distribution of Use Hours for user 58
Actions
Hour
0
100
200
300
400
500
600
700
800
900
0
5
10
15
20
25

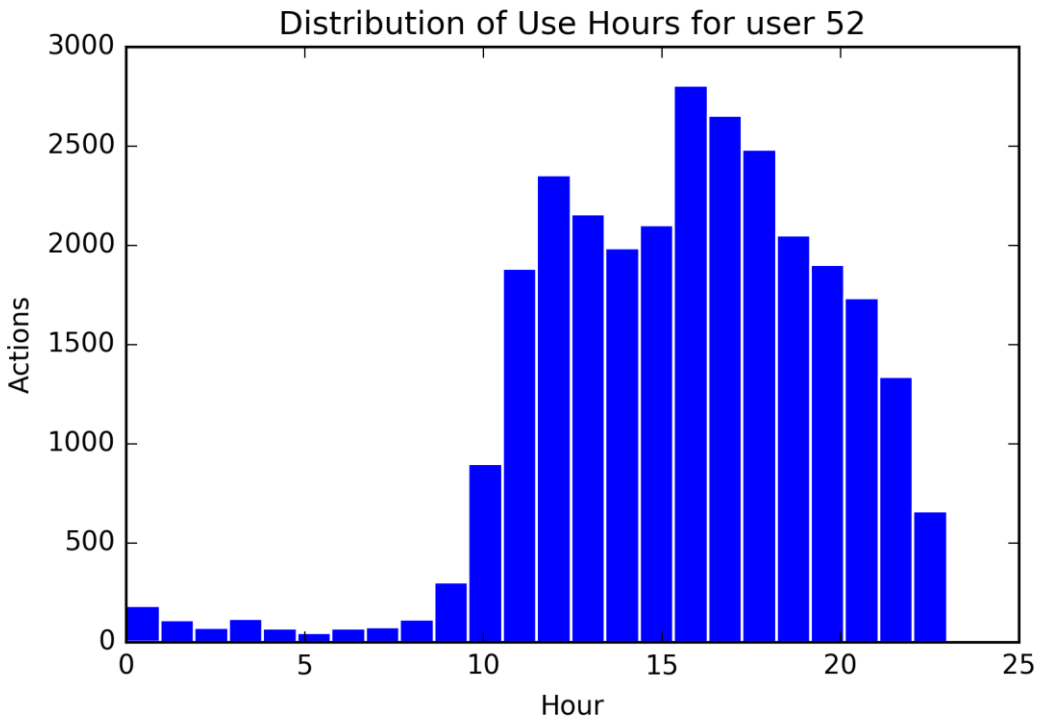

Distribution of Use Hours for user 57
Actions
Hour
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
0
5
10
15
20
25

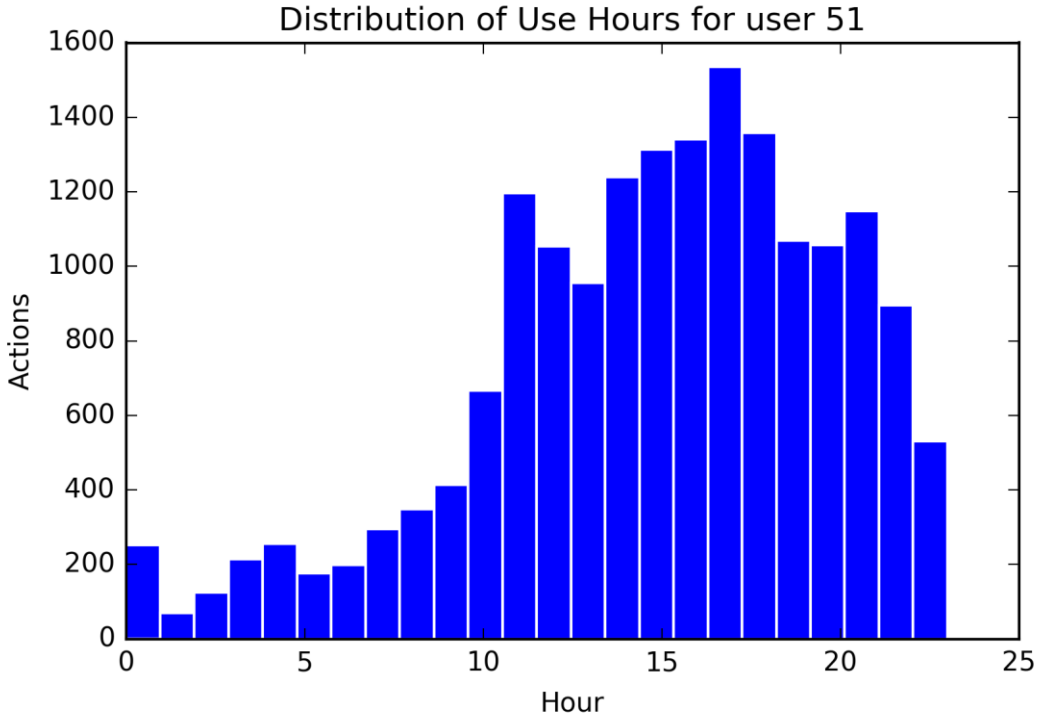

Distribution of Use Hours for user 56
Actions
Hour
0
200
400
600
800
1000
1200
0
5
10
15
20
25

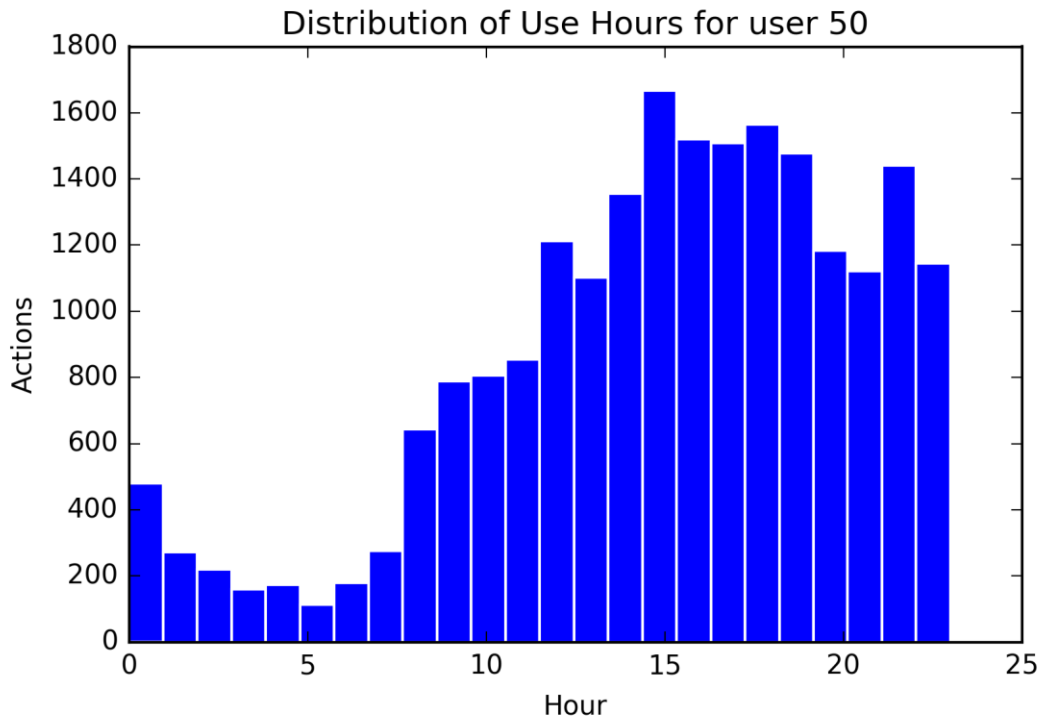

Distribution of Use Hours for user 55
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25

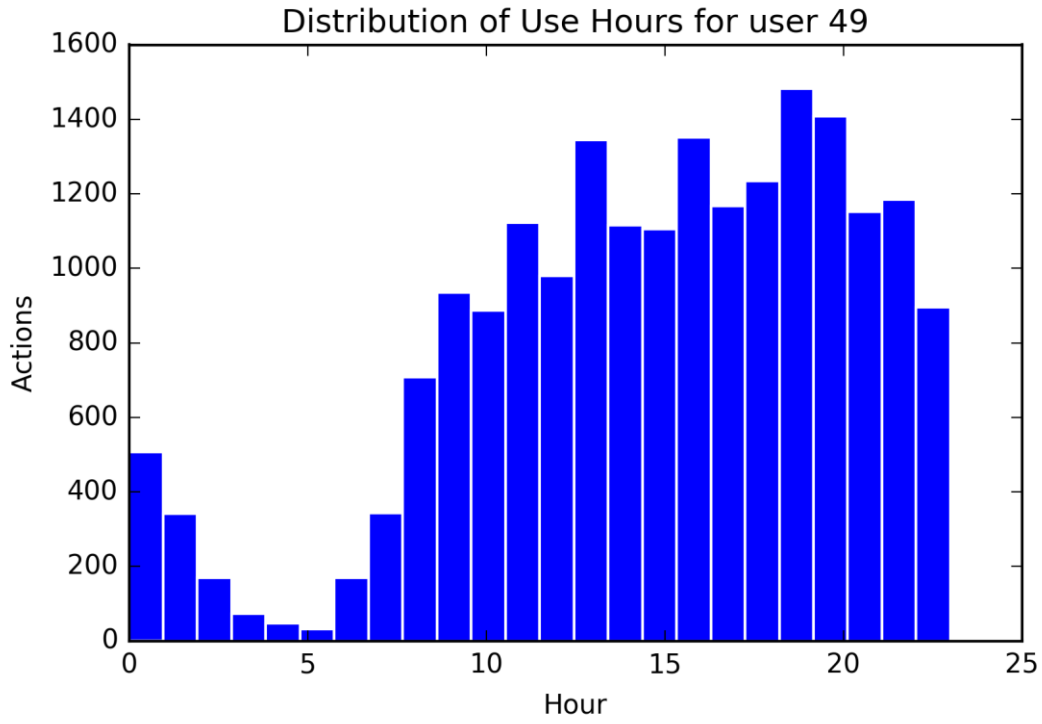

Distribution of Use Hours for user 54
Actions
Hour
0
500
1000
1500
2000
2500
3000
3500
0
5
10
15
20
25

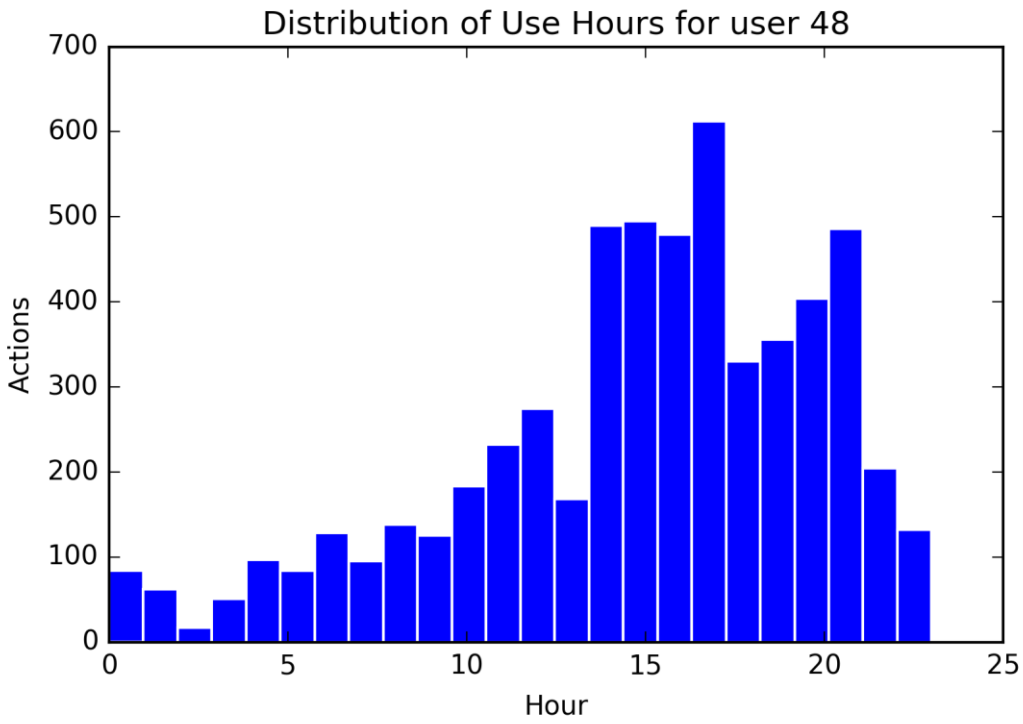

Distribution of Use Hours for user 53
Actions
Hour
0
5000
10000
15000
20000
25000
0
5
10
15
20
25

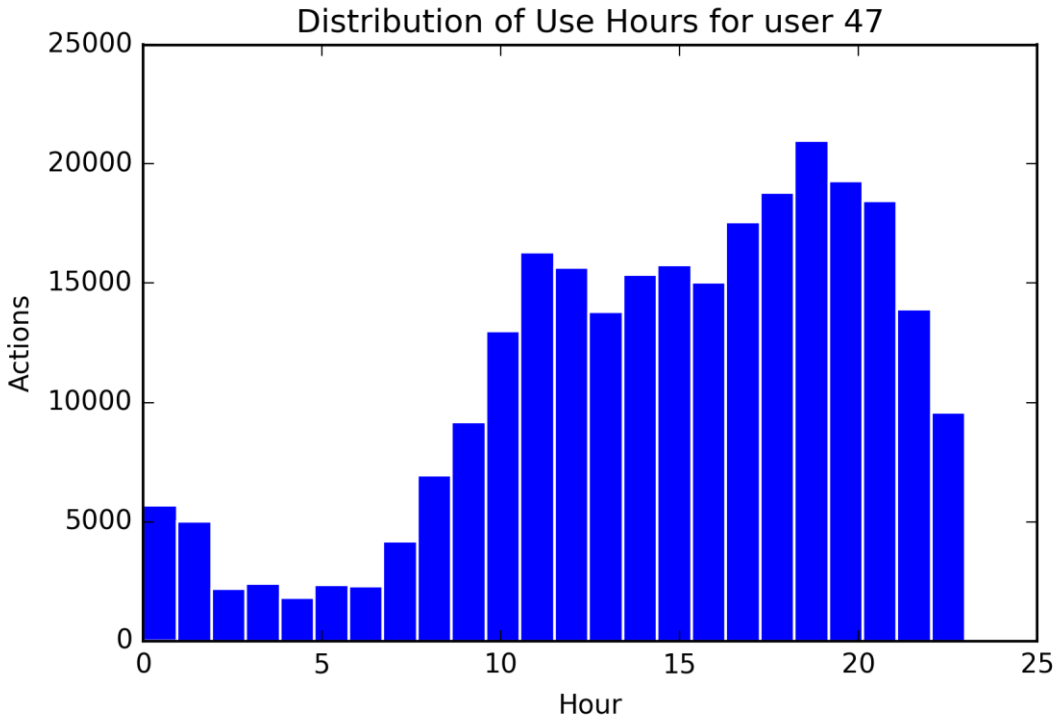

Distribution of Use Hours for user 52
Actions
Hour
0
500
1000
1500
2000
2500
3000
0
5
10
15
20
25

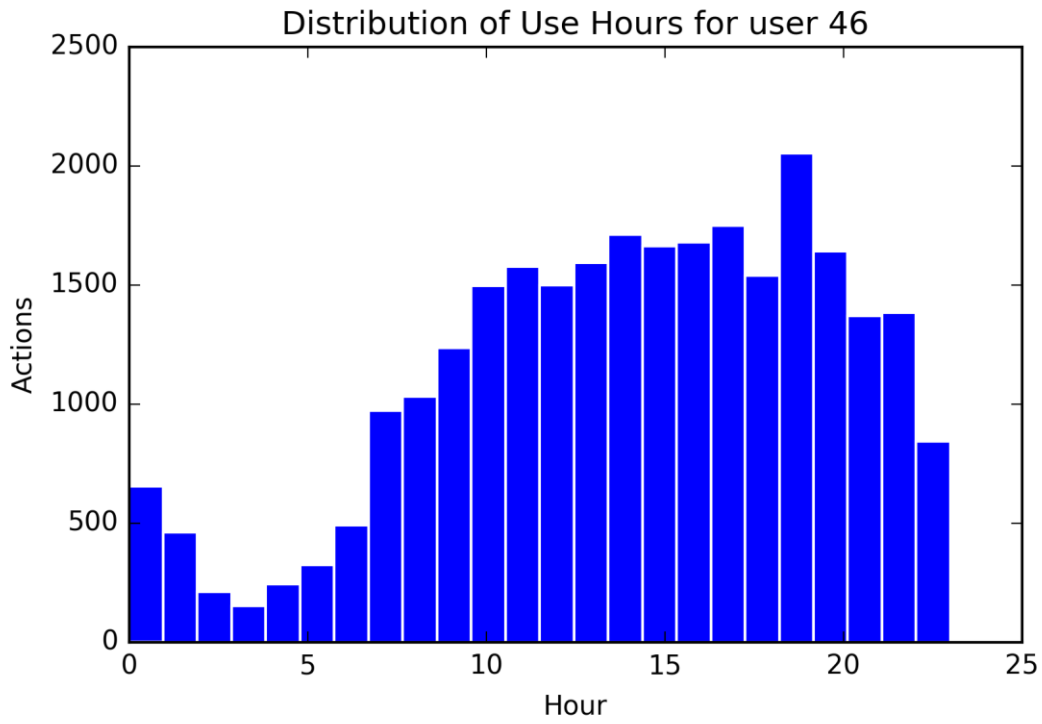

Distribution of Use Hours for user 51
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25

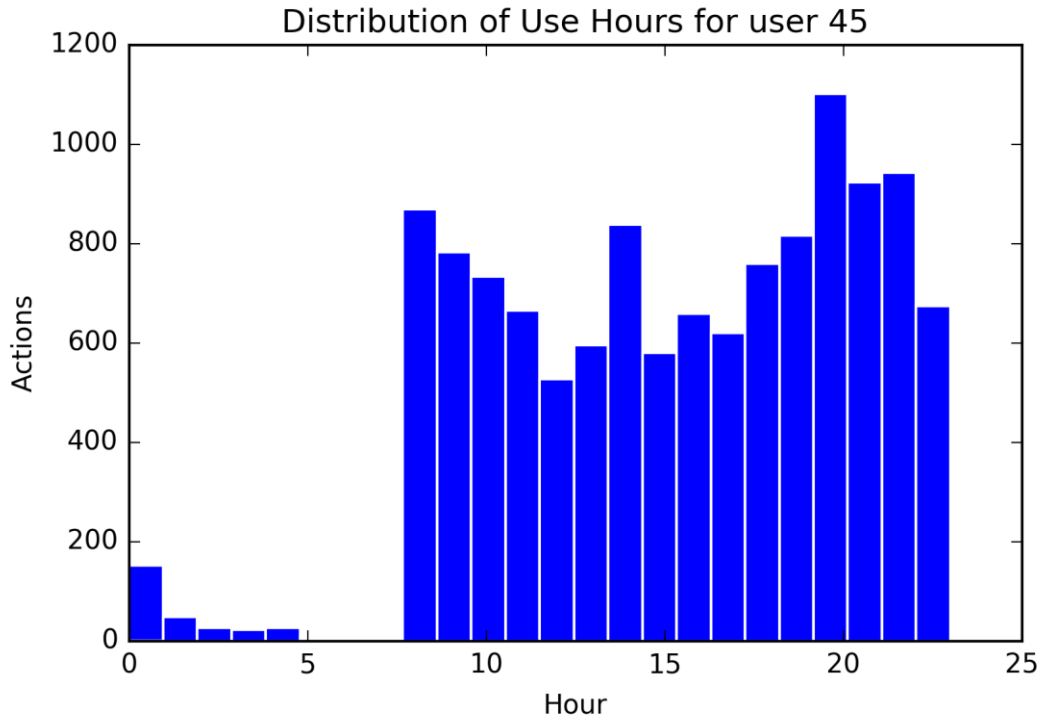

Distribution of Use Hours for user 50
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
1800
0
5
10
15
20
25

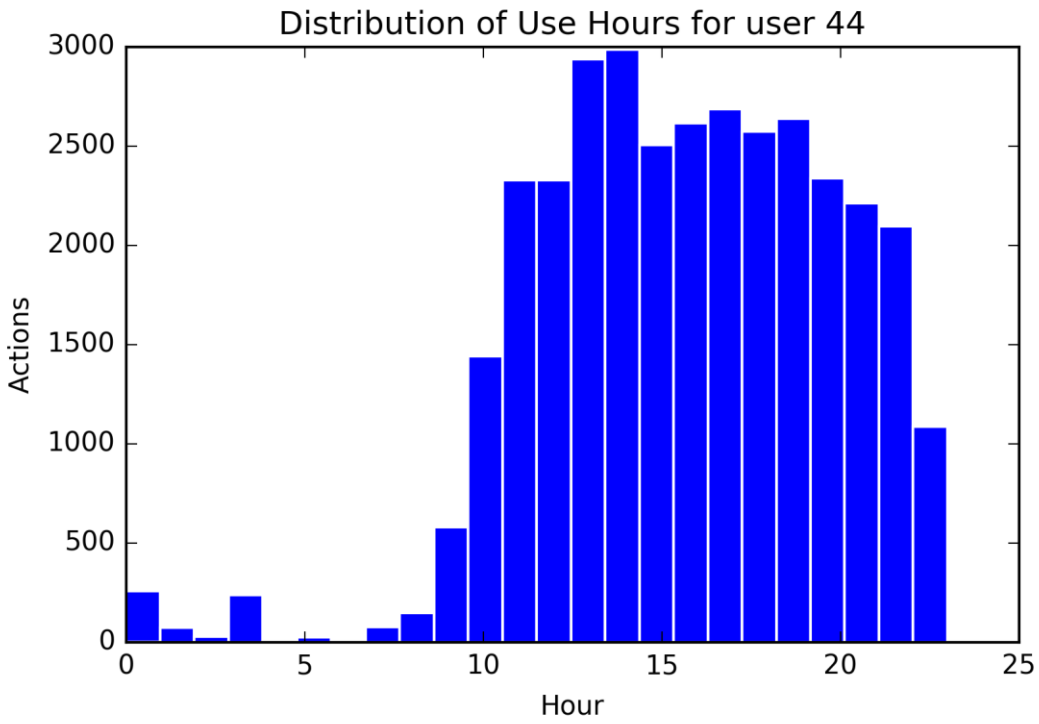

Distribution of Use Hours for user 49
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25

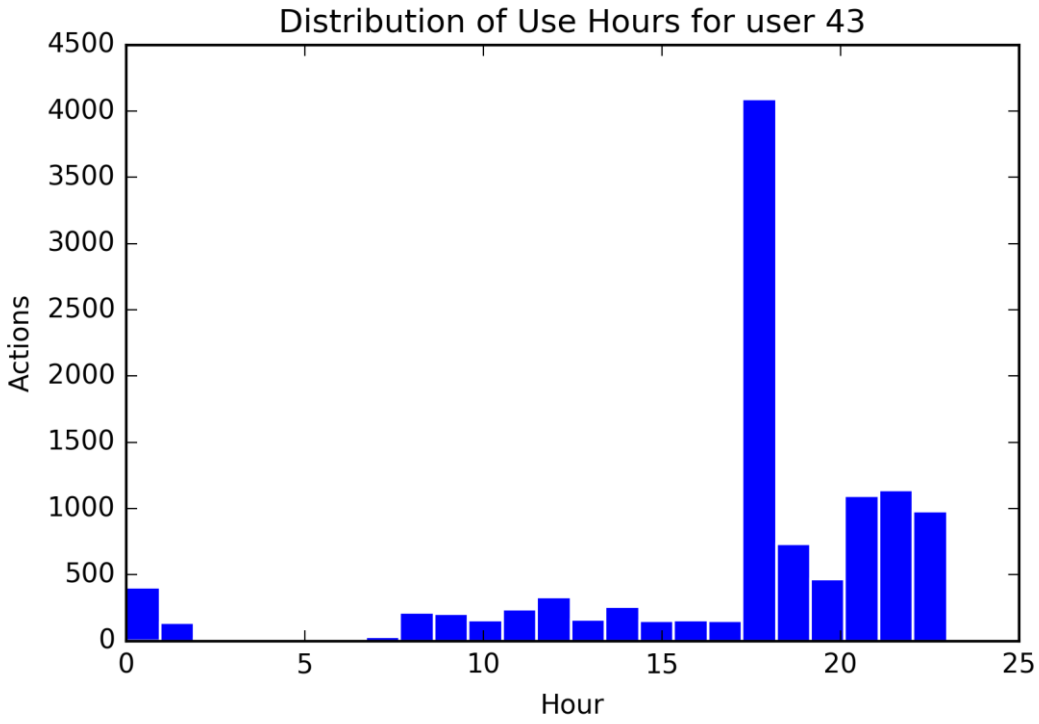

Distribution of Use Hours for user 48
Actions
Hour
0
100
200
300
400
500
600
700
0
5
10
15
20
25

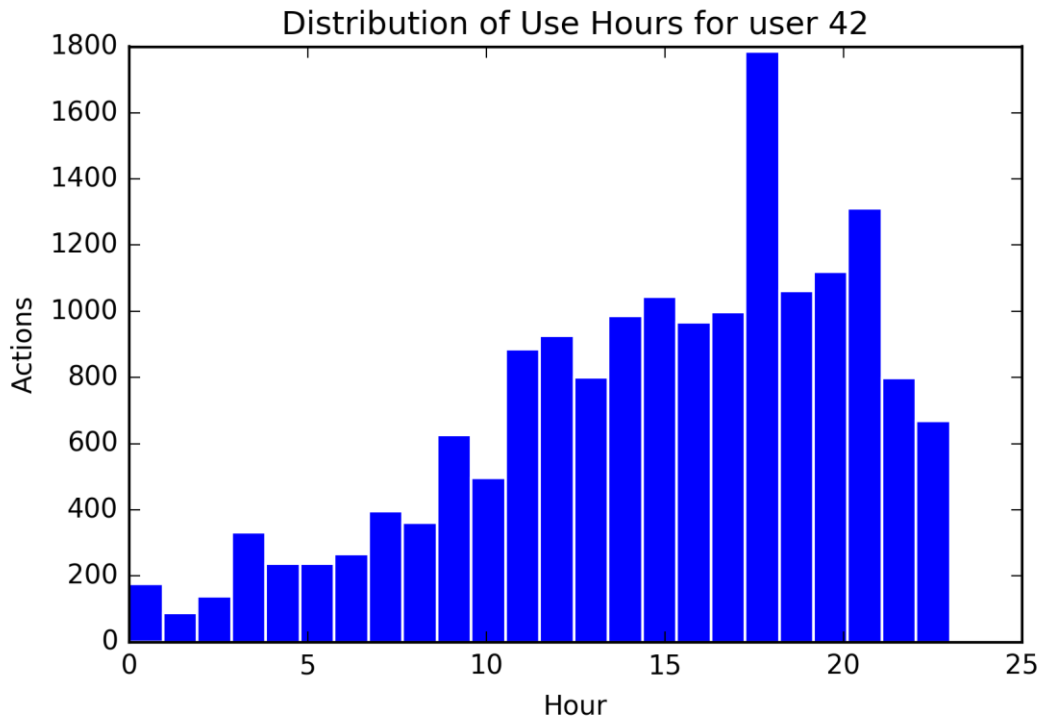

Distribution of Use Hours for user 47
Actions
Hour
0
5000
10000
15000
20000
25000
0
5
10
15
20
25

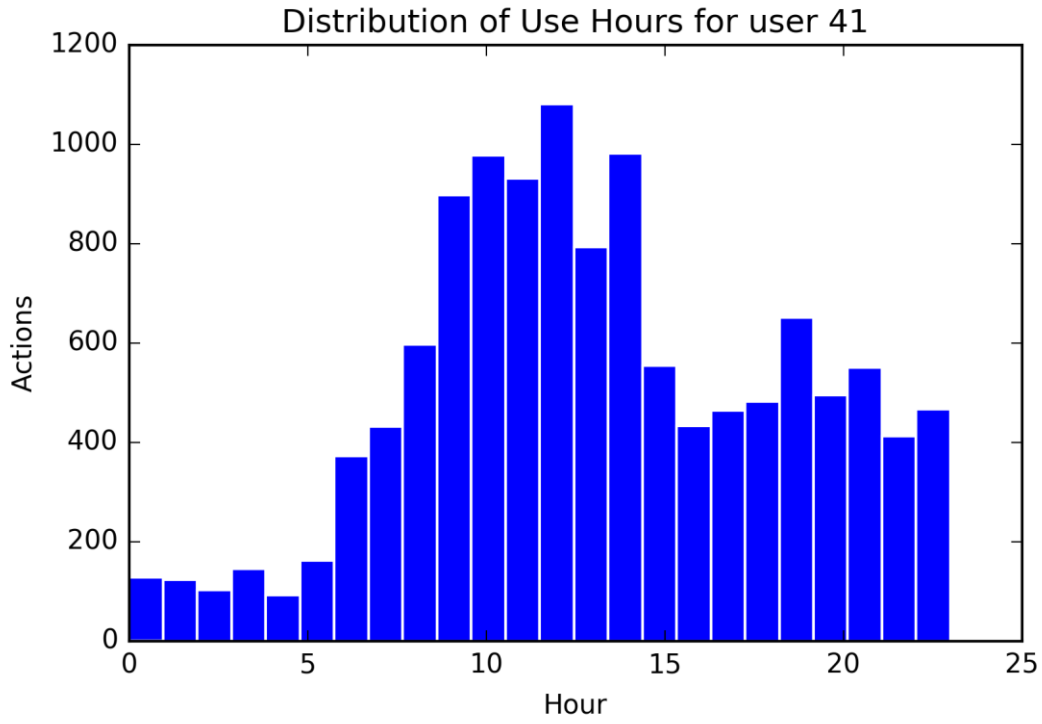

Distribution of Use Hours for user 46
Actions
Hour
0
500
1000
1500
2000
2500
0
5
10
15
20
25

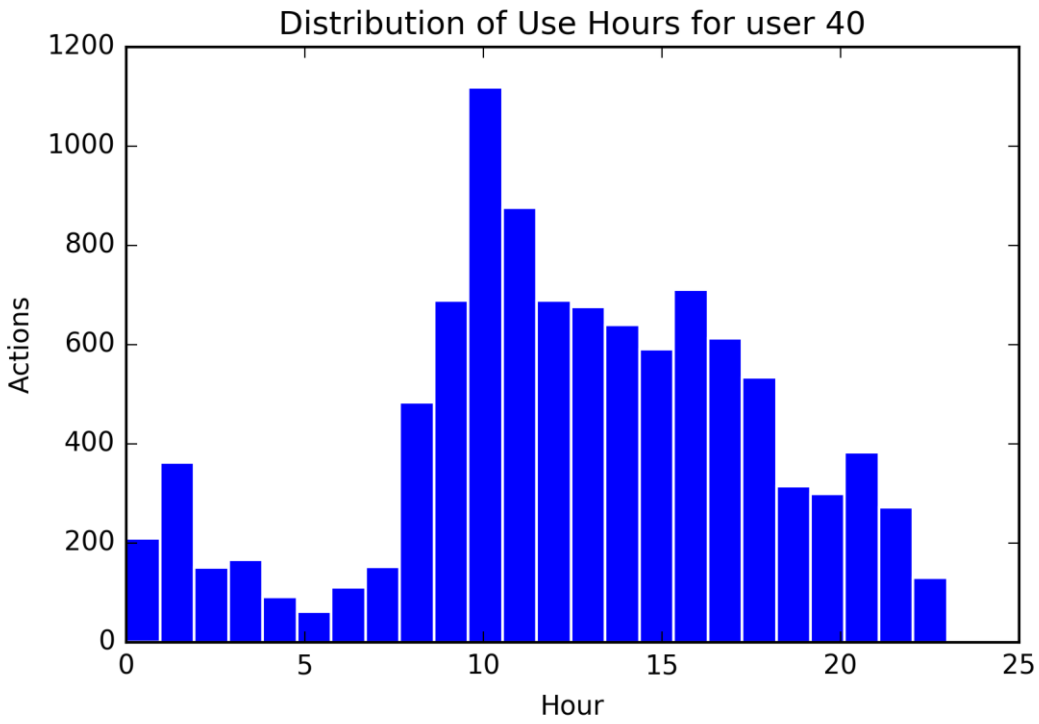

Distribution of Use Hours for user 45
Actions
Hour
0
200
400
600
800
1000
1200
0
5
10
15
20
25

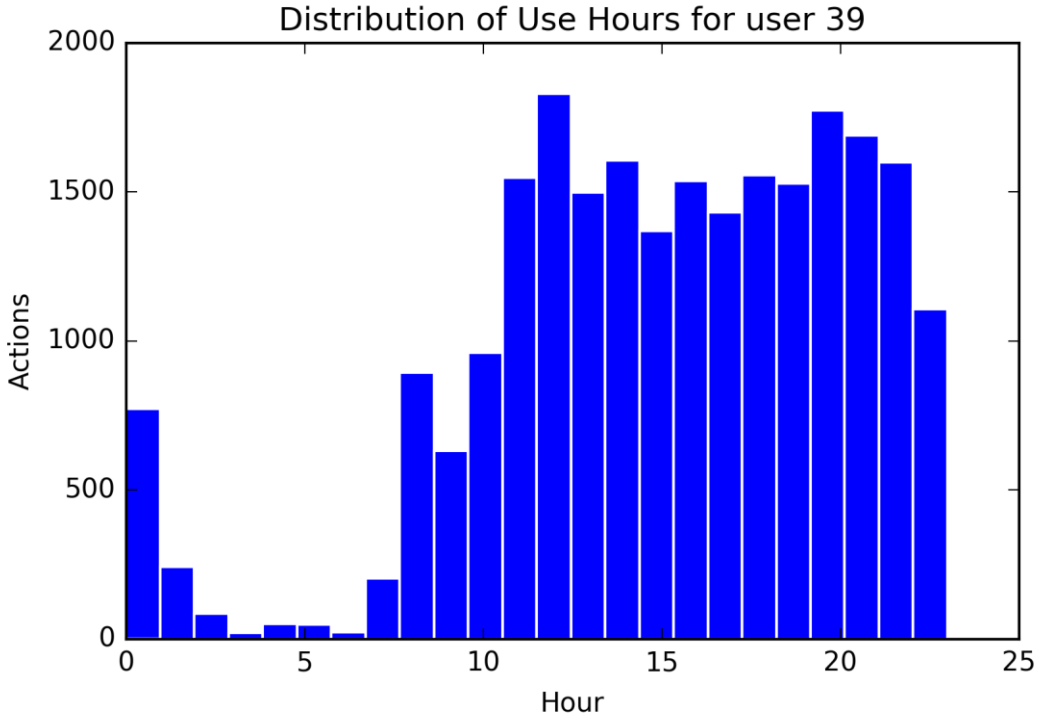

Distribution of Use Hours for user 44
Actions
Hour
0
500
1000
1500
2000
2500
3000
0
5
10
15
20
25

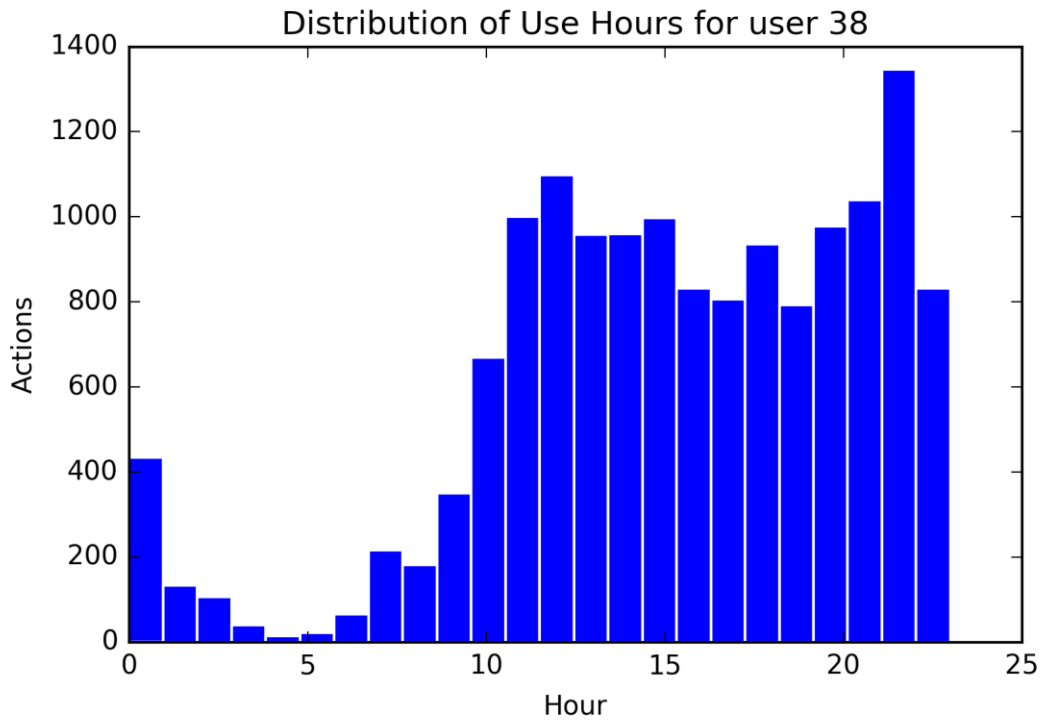

Distribution of Use Hours for user 43
Actions
Hour
0
500
1000
1500
2000
2500
3000
3500
4000
4500
0
5
10
15
20
25

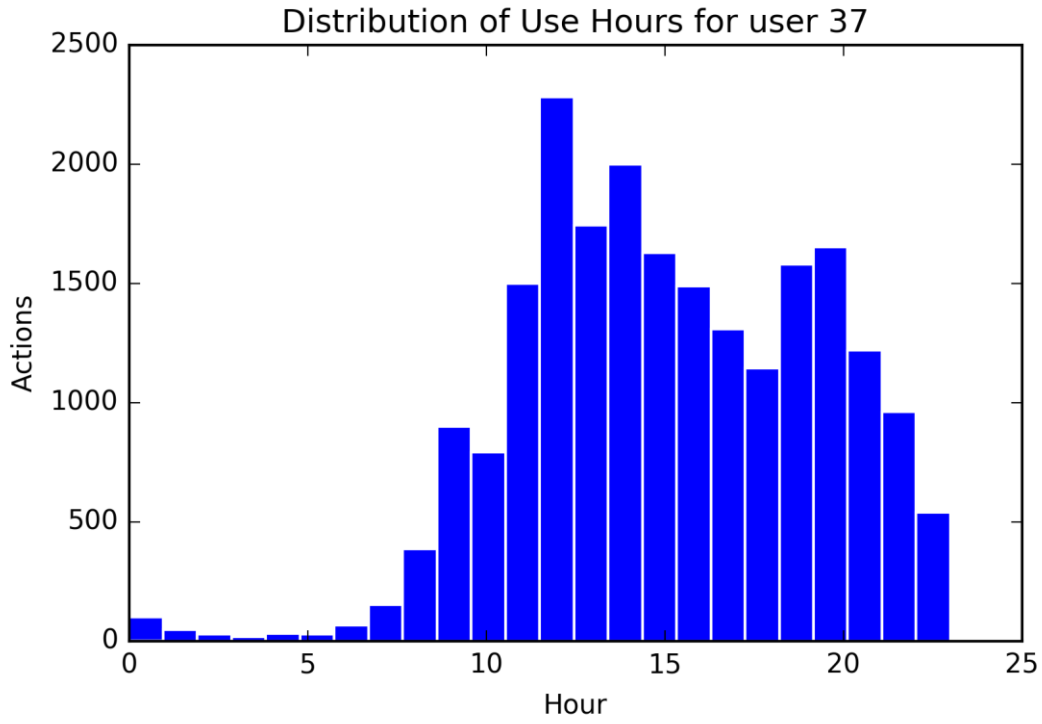

Distribution of Use Hours for user 42
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
1800
0
5
10
15
20
25

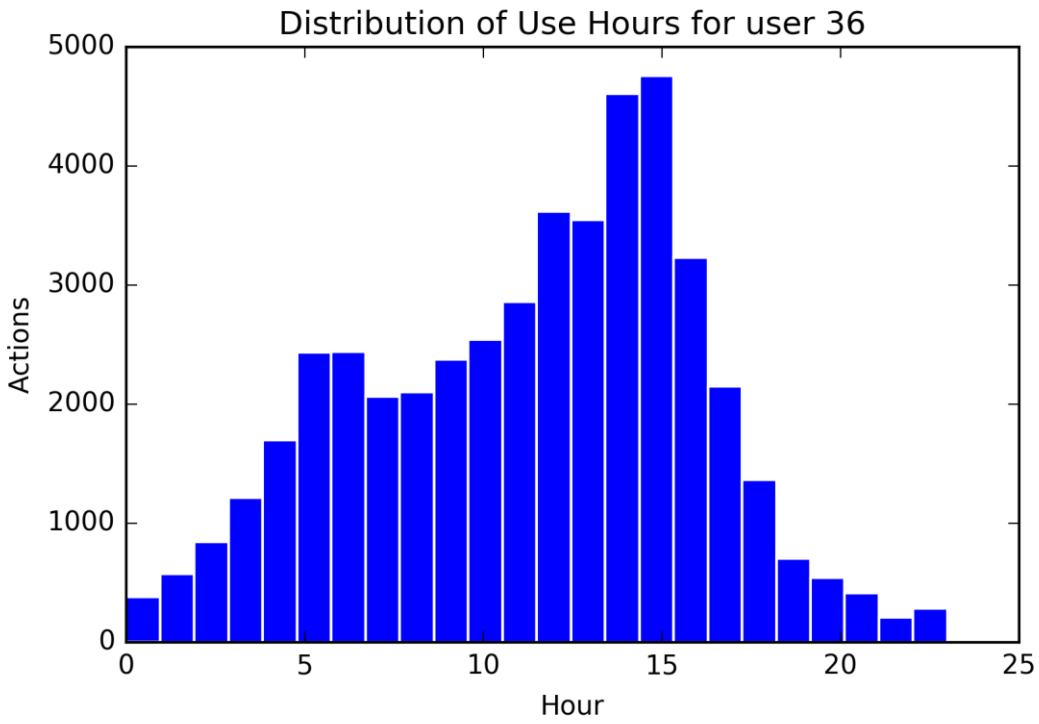

Distribution of Use Hours for user 41
Actions
Hour
0
200
400
600
800
1000
1200
0
5
10
15
20
25

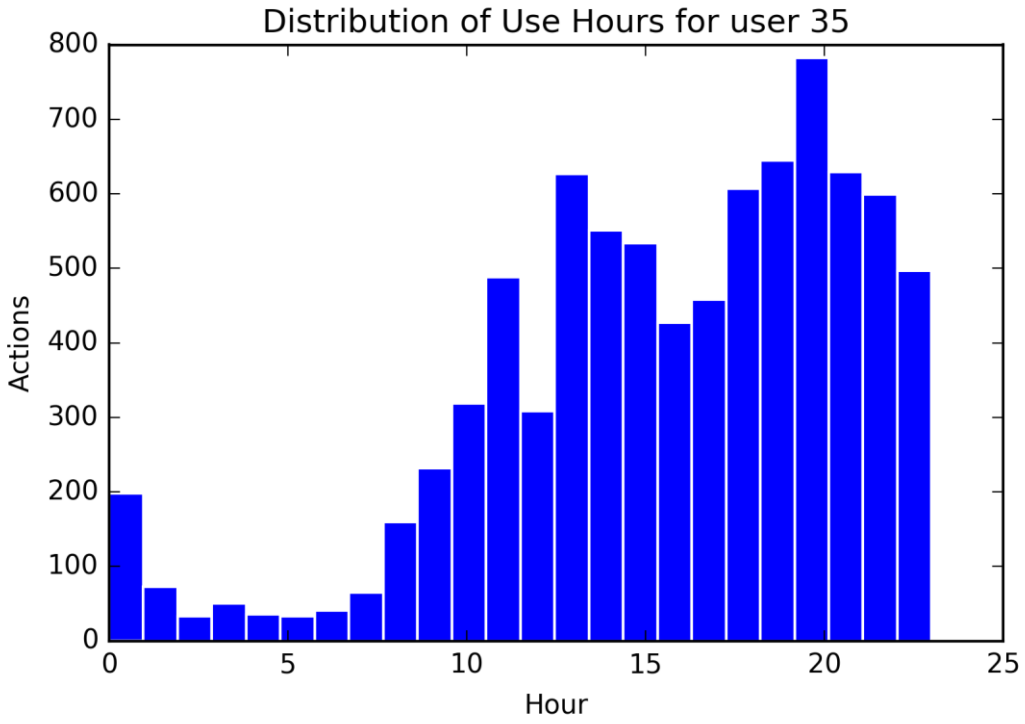

Distribution of Use Hours for user 40
Actions
Hour
0
200
400
600
800
1000
1200
0
5
10
15
20
25

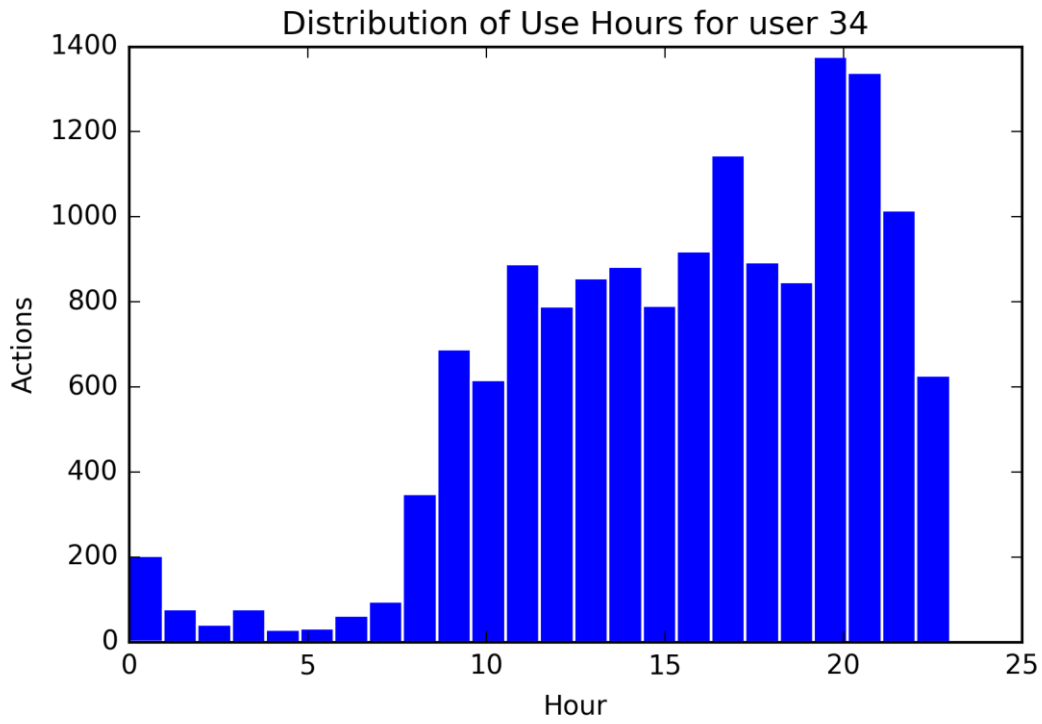

Distribution of Use Hours for user 39
Actions
Hour
0
500
1000
1500
2000
0
5
10
15
20
25

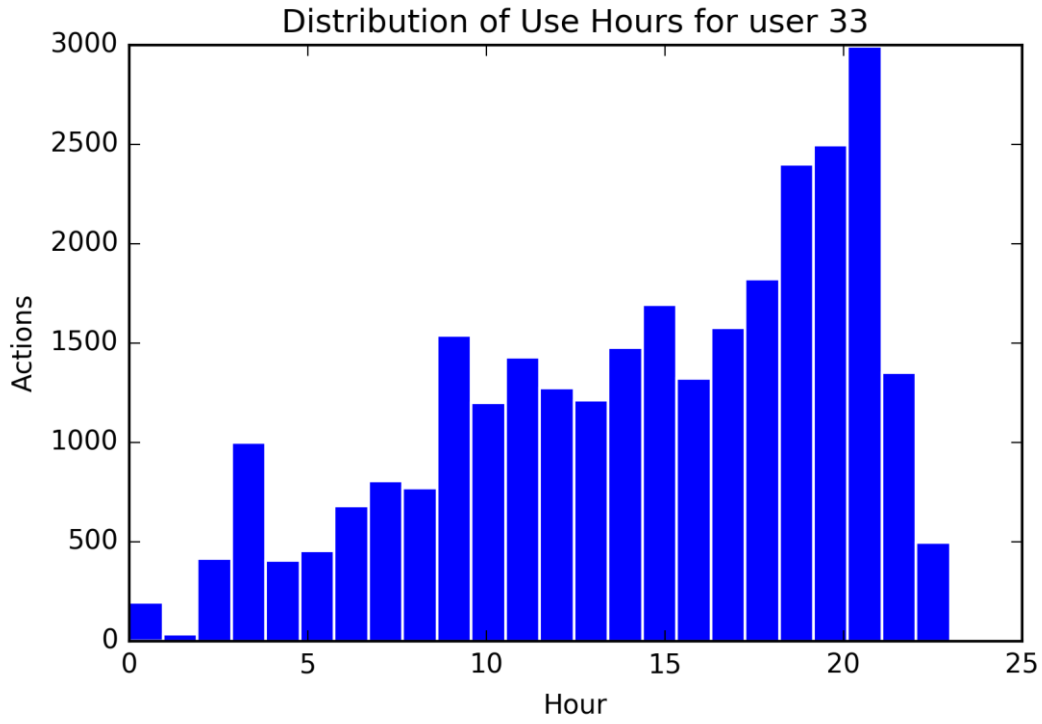

Distribution of Use Hours for user 38
Actions
Hour
0
200
400
600
800
1000
1200
1400
0
5
10
15
20
25

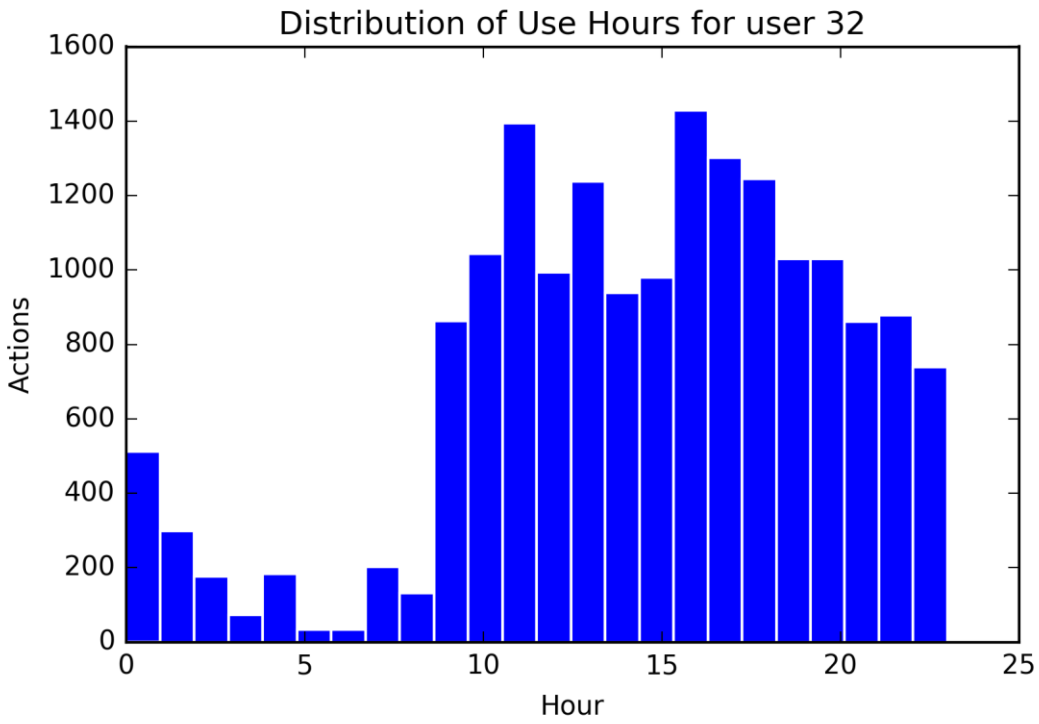

Distribution of Use Hours for user 37
Actions
Hour
0
500
1000
1500
2000
2500
0
5
10
15
20
25

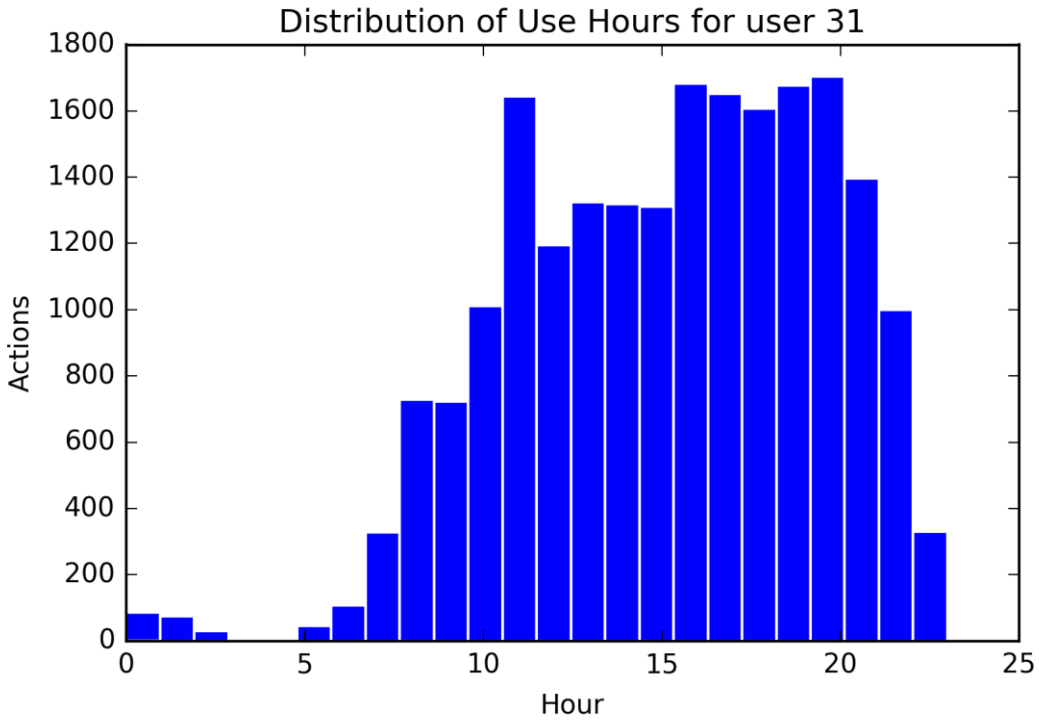

Distribution of Use Hours for user 36
Actions
Hour
0
1000
2000
3000
4000
5000
0
5
10
15
20
25

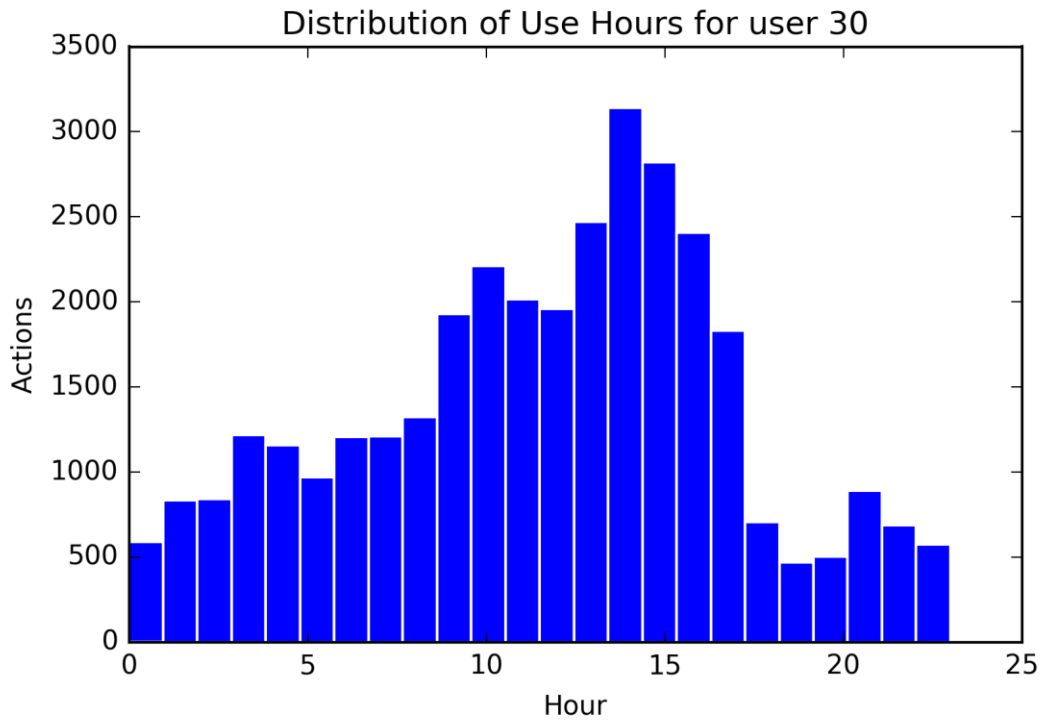

Distribution of Use Hours for user 35
Actions
Hour
0
100
200
300
400
500
600
700
800
0
5
10
15
20
25

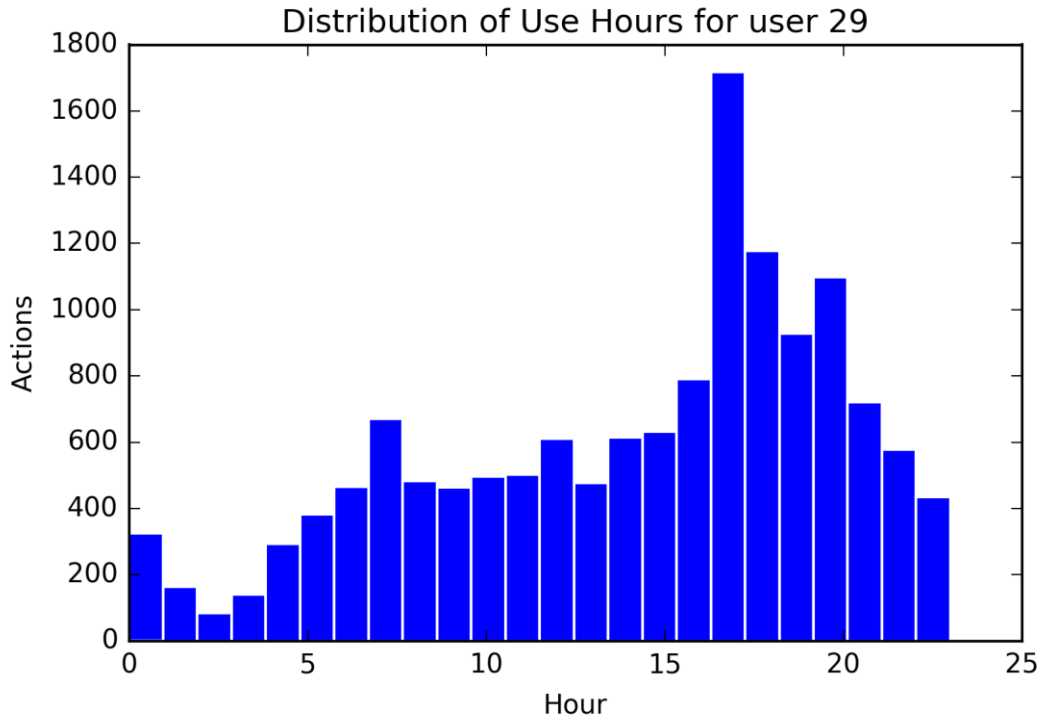

Distribution of Use Hours for user 34
Actions
Hour
0
200
400
600
800
1000
1200
1400
0
5
10
15
20
25

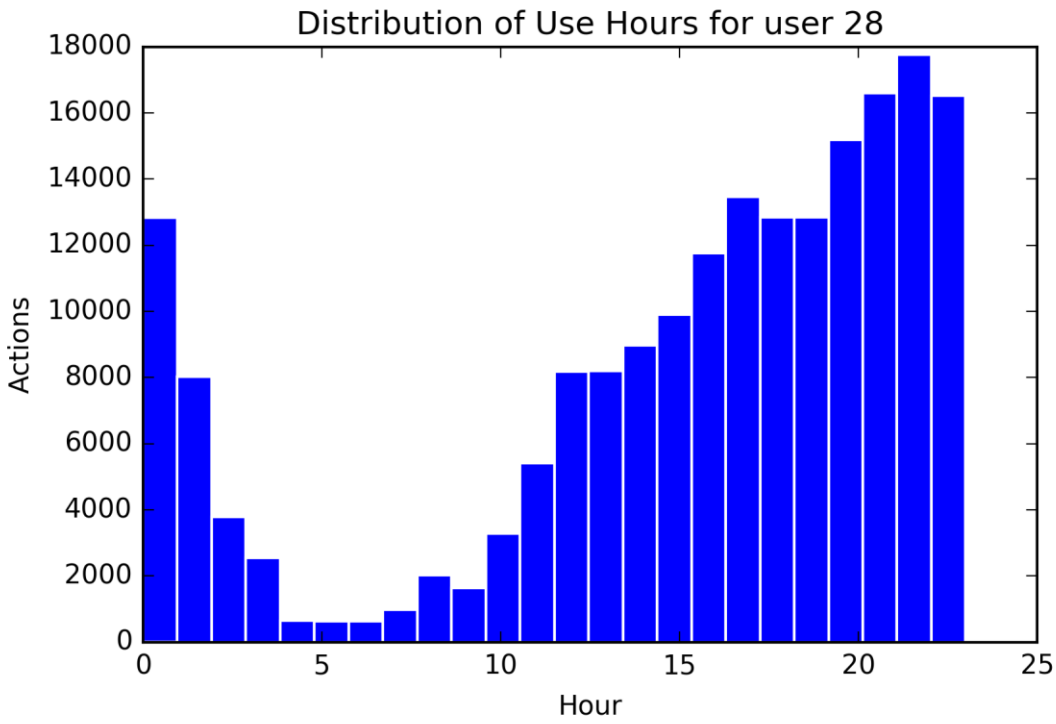

Distribution of Use Hours for user 33
Actions
Hour
0
500
1000
1500
2000
2500
3000
0
5
10
15
20
25

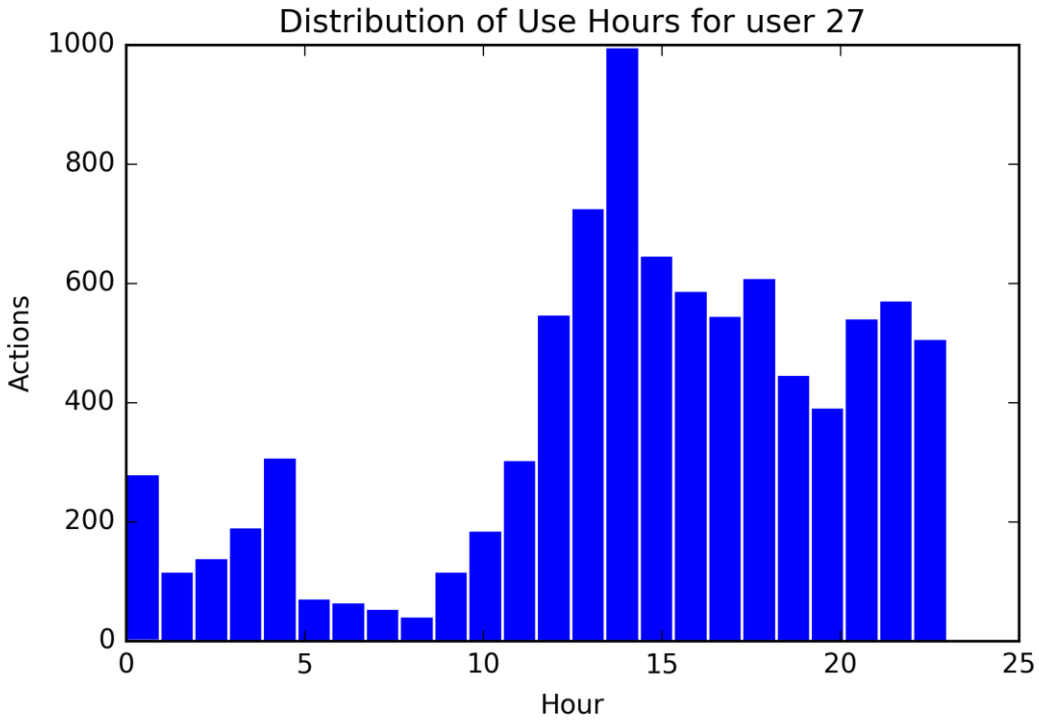

Distribution of Use Hours for user 32
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25

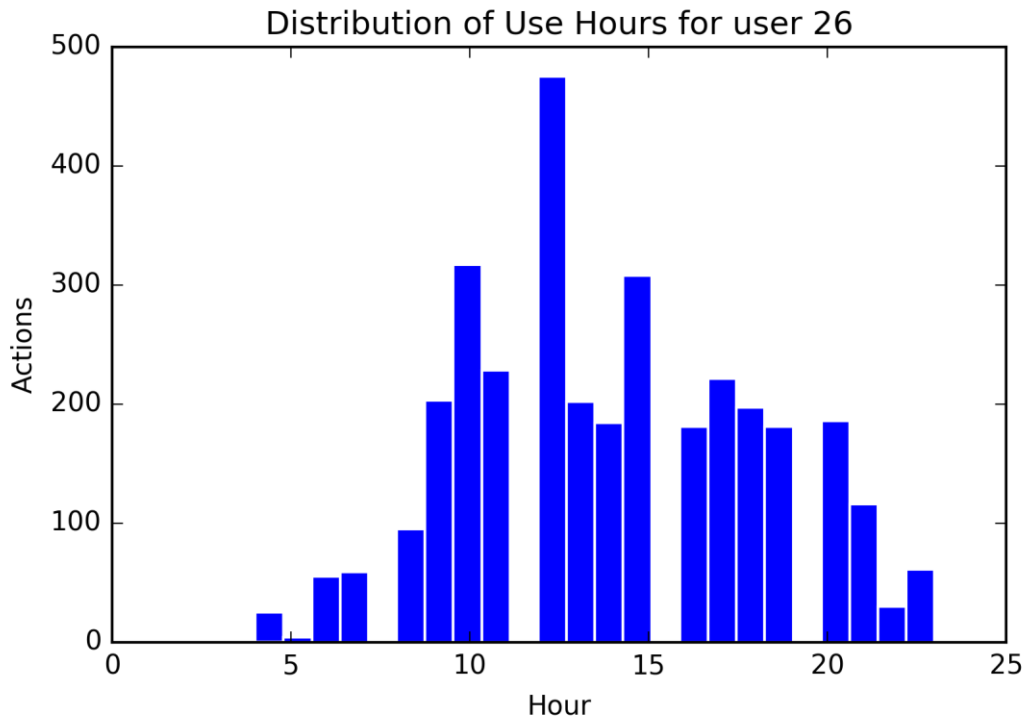

Distribution of Use Hours for user 31
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
1800
0
5
10
15
20
25

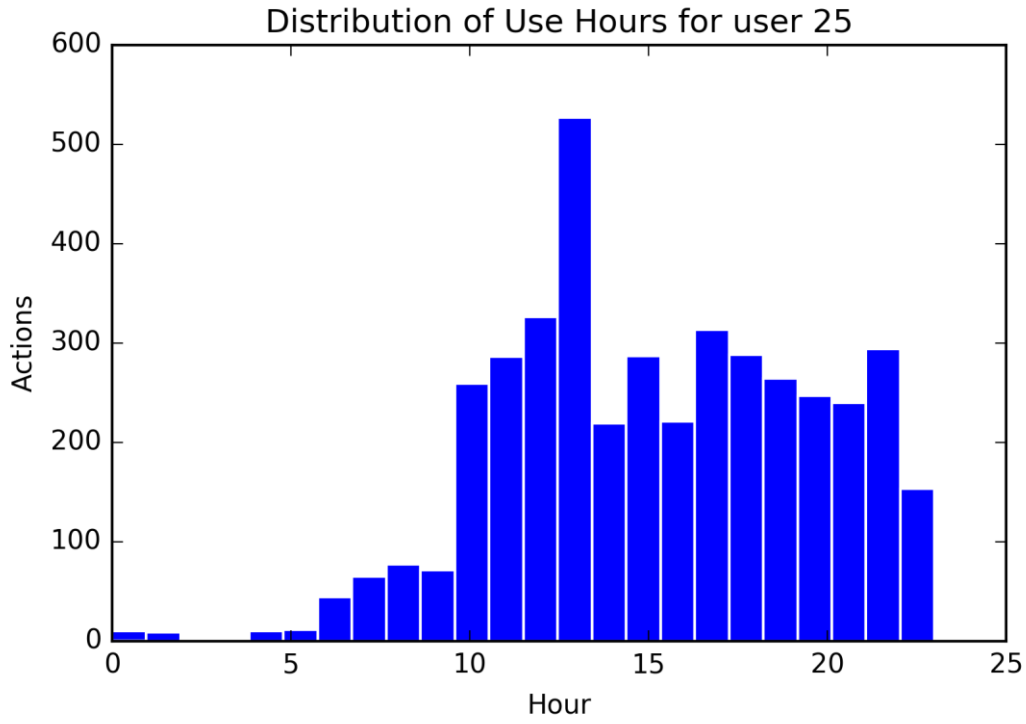

Distribution of Use Hours for user 30
Actions
Hour
0
500
1000
1500
2000
2500
3000
3500
0
5
10
15
20
25

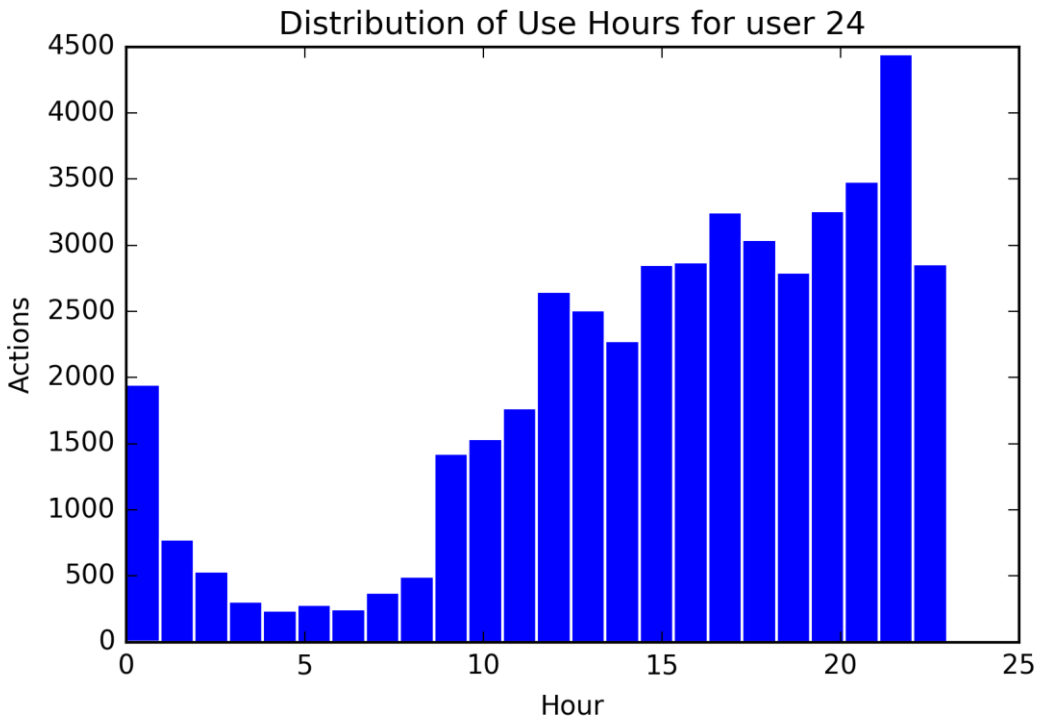

Distribution of Use Hours for user 29
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
1800
0
5
10
15
20
25

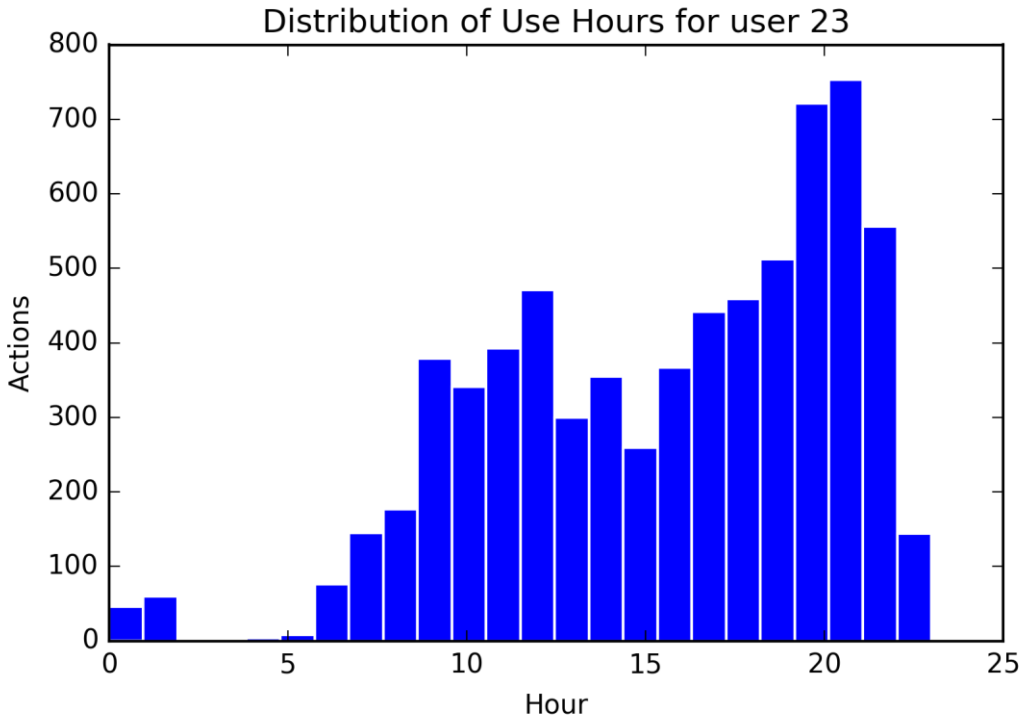

Distribution of Use Hours for user 28
Actions
Hour
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
0
5
10
15
20
25

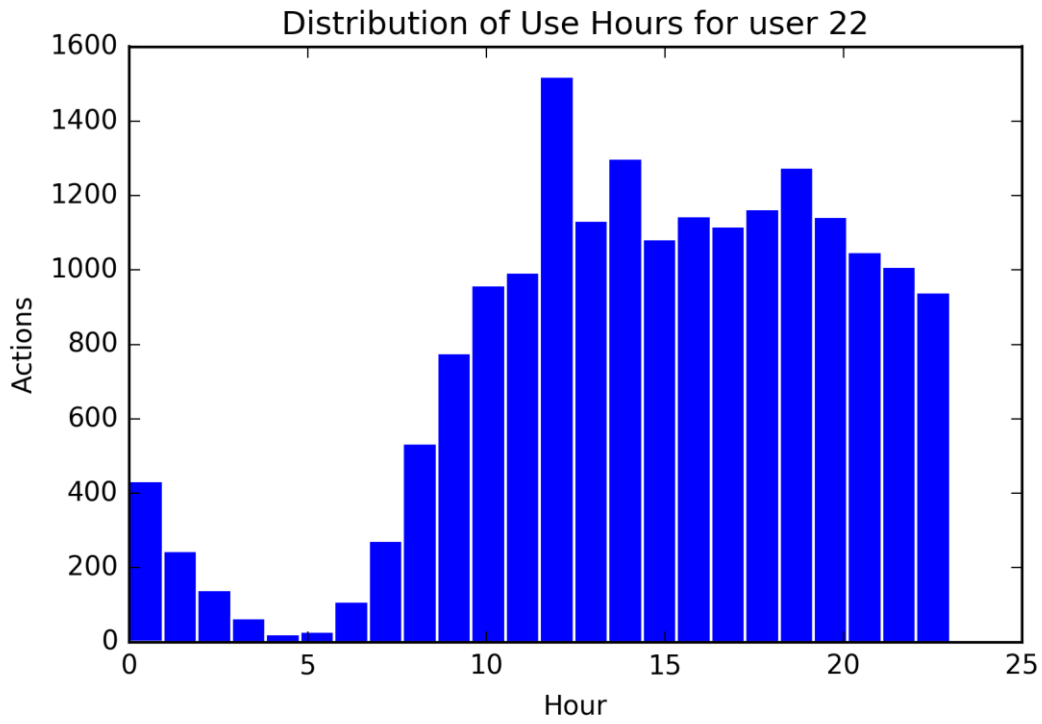

Distribution of Use Hours for user 27
Actions
Hour
0
200
400
600
800
1000
0
5
10
15
20
25

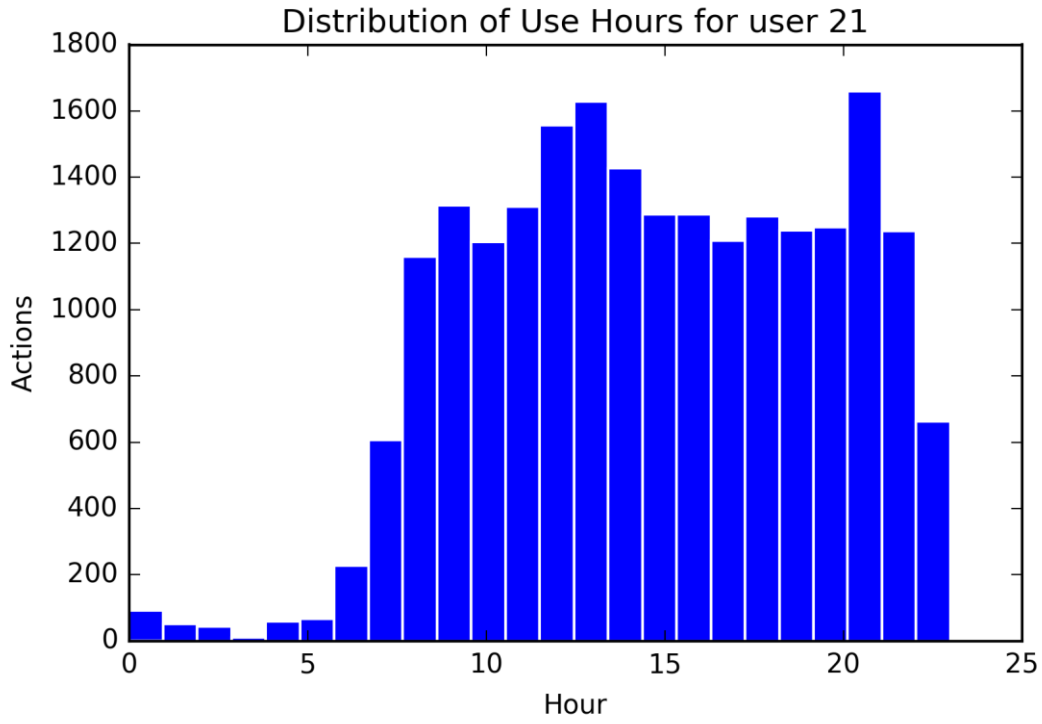

Distribution of Use Hours for user 26
Actions
Hour
0
100
200
300
400
500
0
5
10
15
20
25

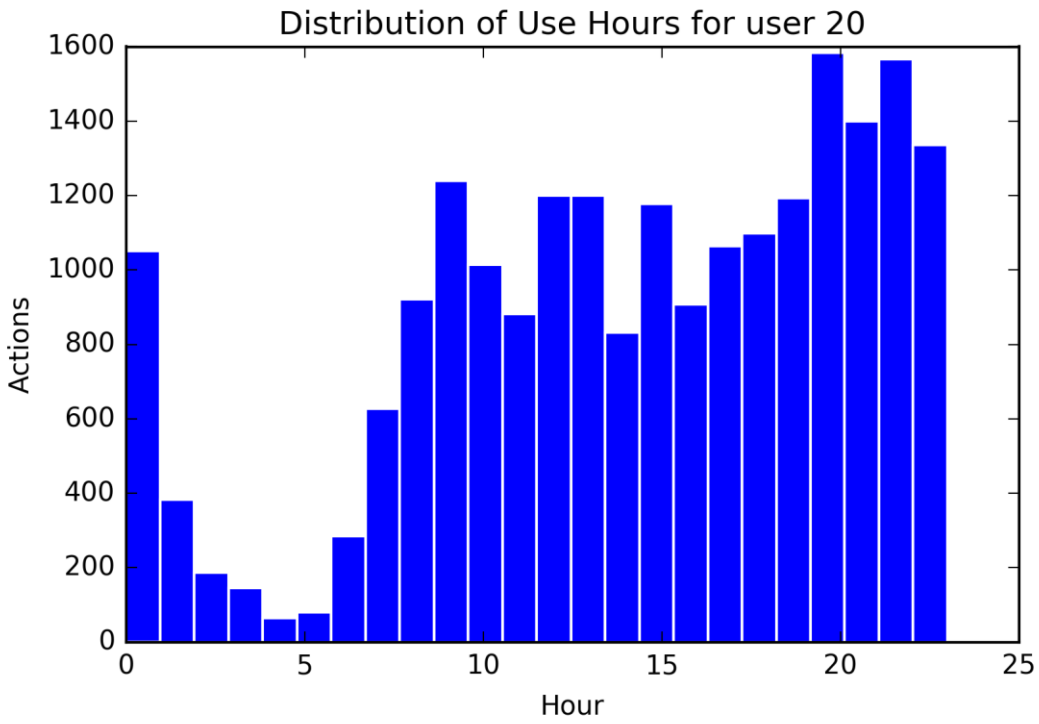

Distribution of Use Hours for user 25
Actions
Hour
0
100
200
300
400
500
600
0
5
10
15
20
25

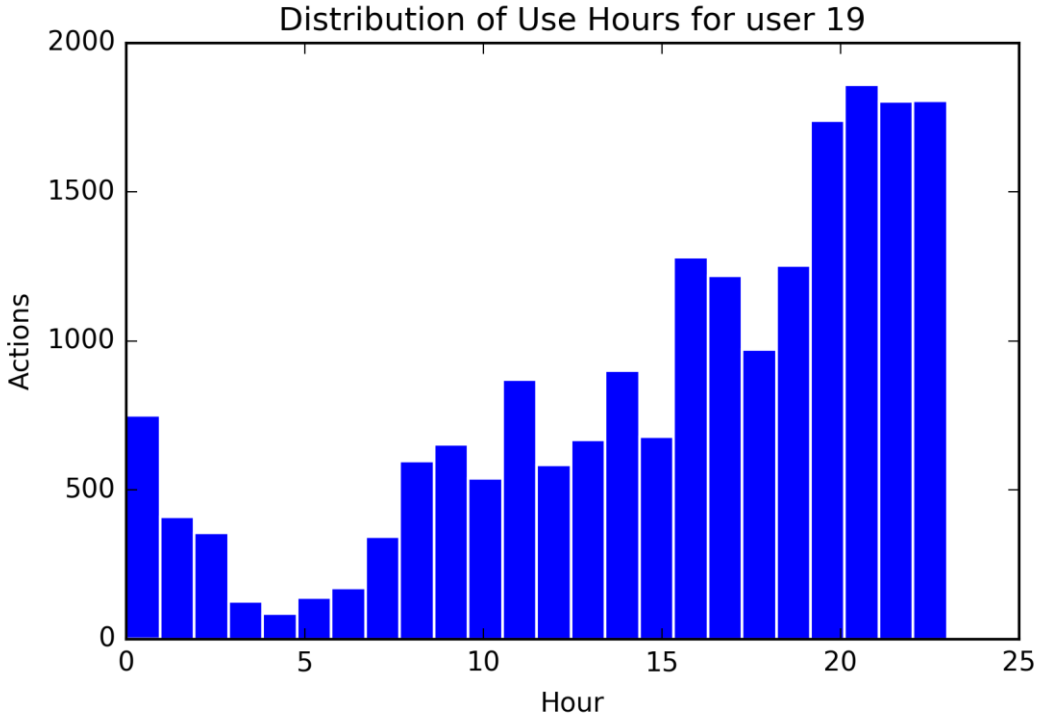

Distribution of Use Hours for user 24
Actions
Hour
0
500
1000
1500
2000
2500
3000
3500
4000
4500
0
5
10
15
20
25

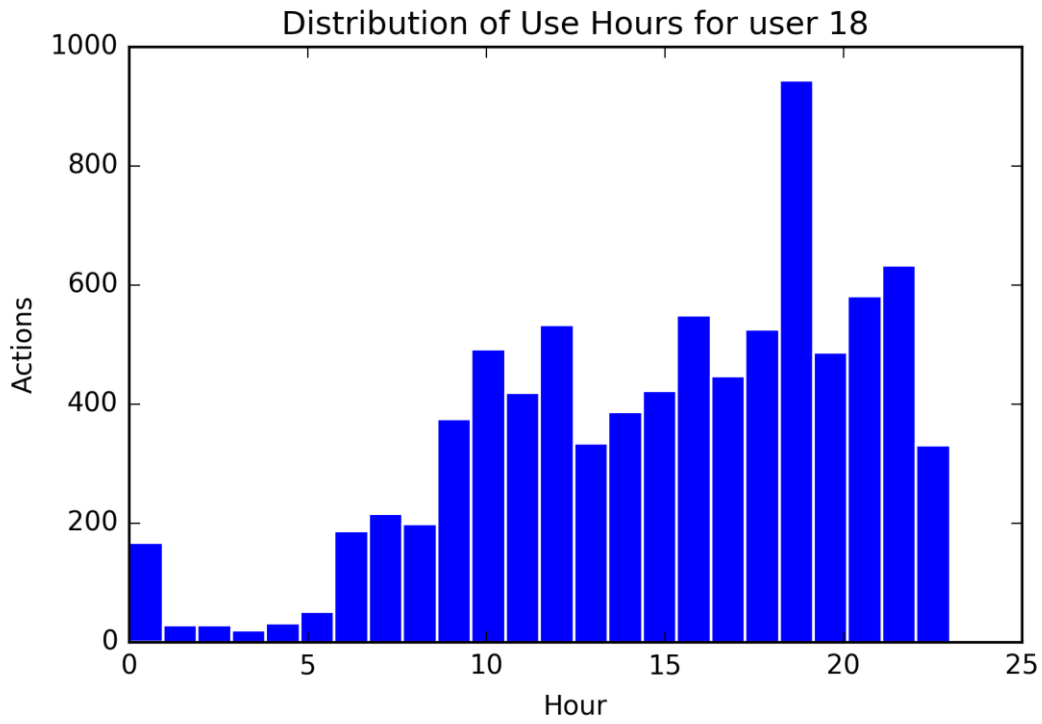

Distribution of Use Hours for user 23
Actions
Hour
0
100
200
300
400
500
600
700
800
0
5
10
15
20
25

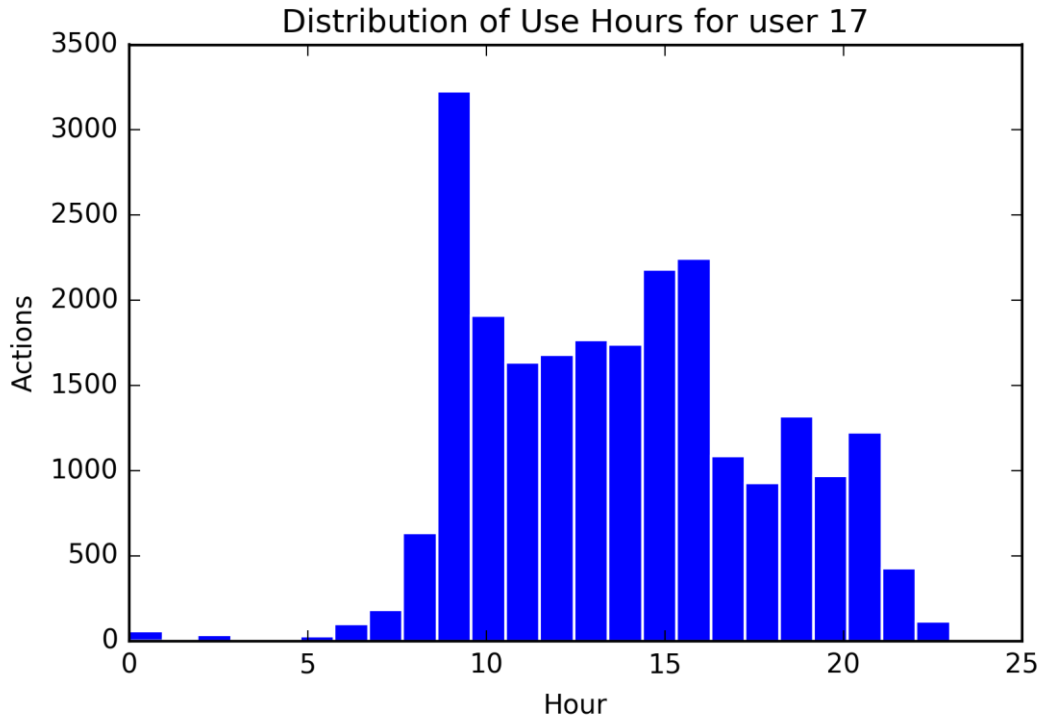

Distribution of Use Hours for user 22
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25

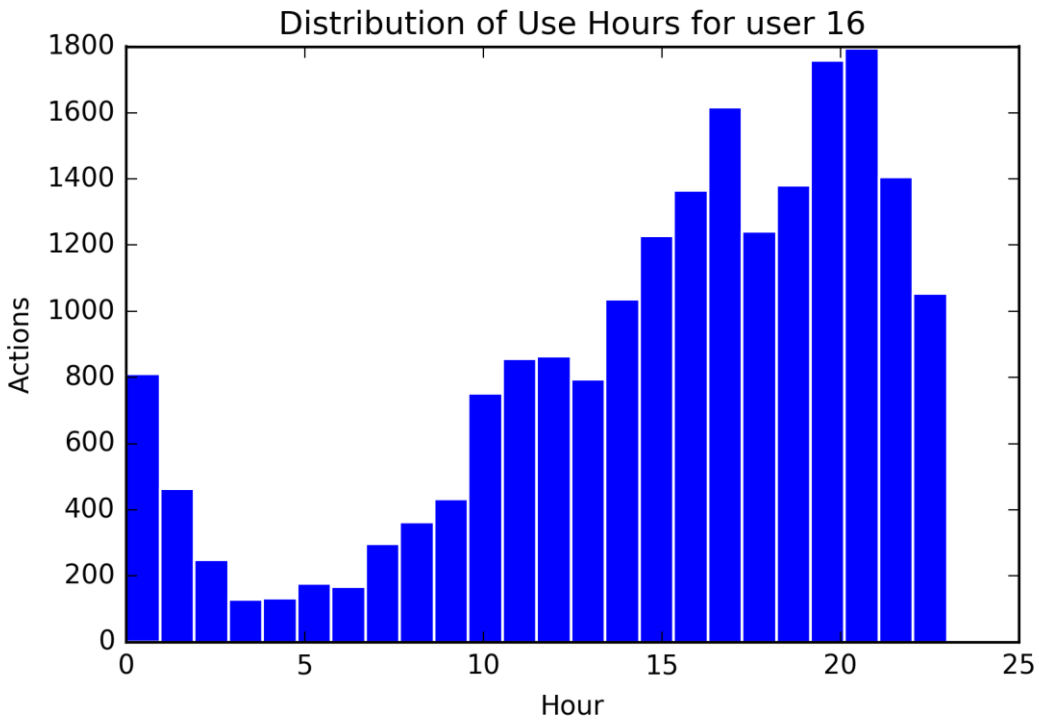

Distribution of Use Hours for user 21
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
1800
0
5
10
15
20
25

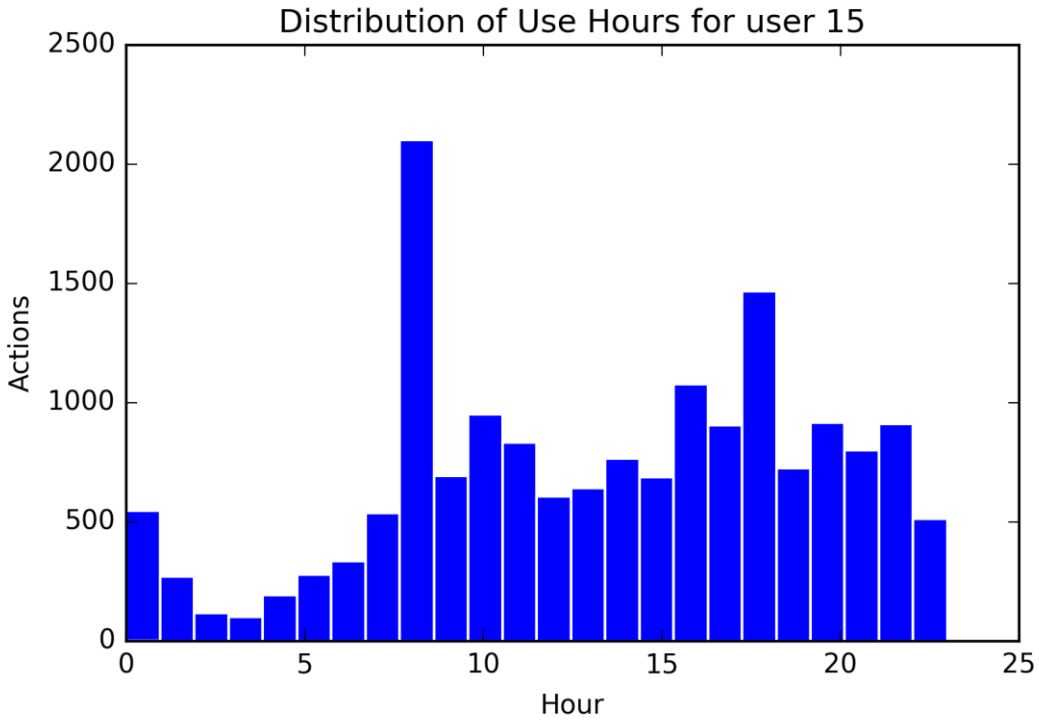

Distribution of Use Hours for user 20
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25

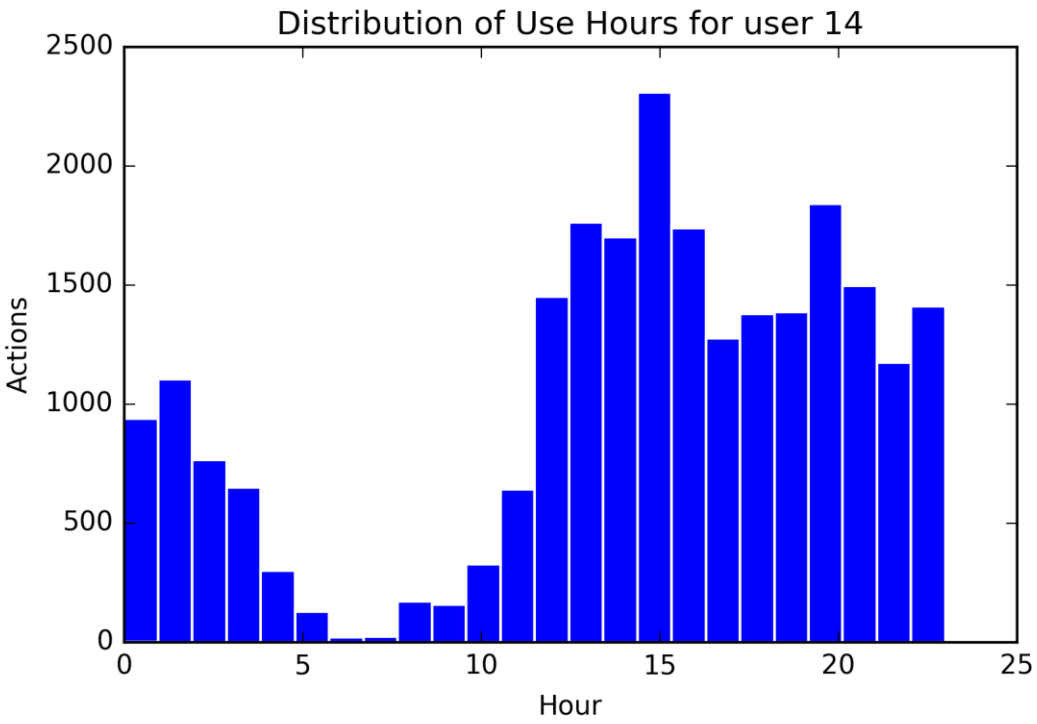

Distribution of Use Hours for user 19
Actions
Hour
0
500
1000
1500
2000
0
5
10
15
20
25

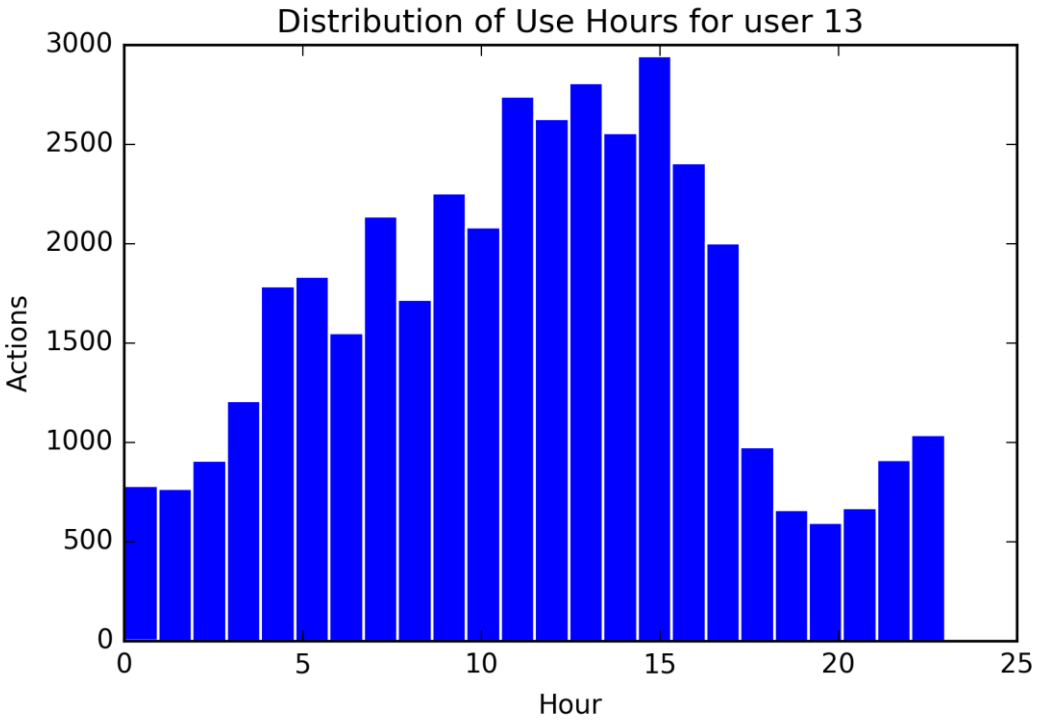

Distribution of Use Hours for user 18
Actions
Hour
0
200
400
600
800
1000
0
5
10
15
20
25

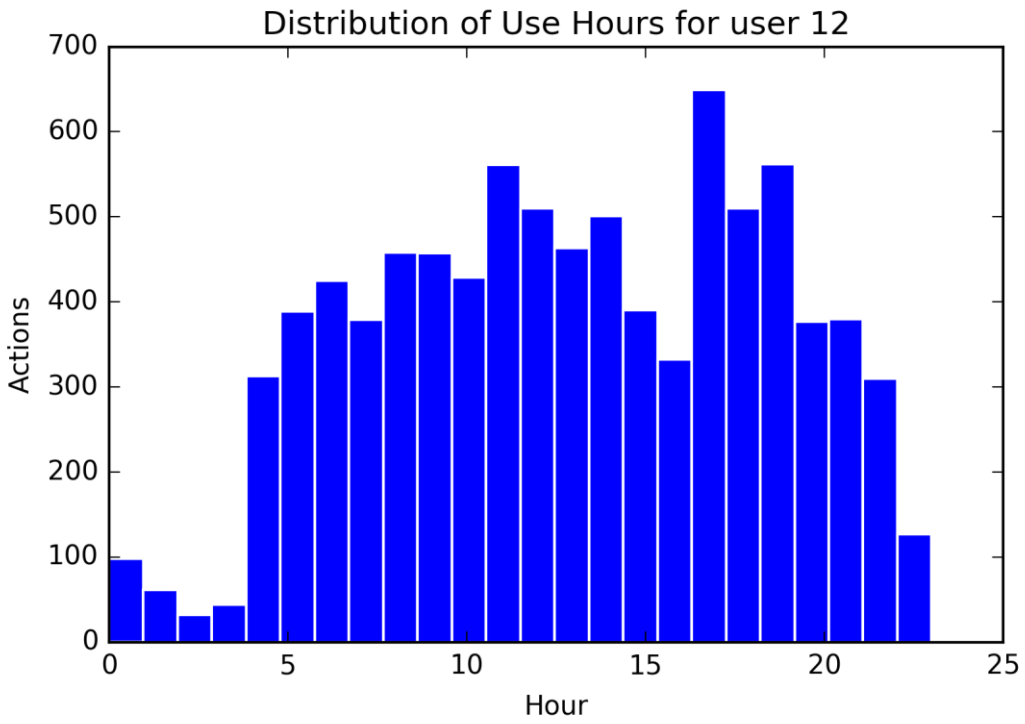

Distribution of Use Hours for user 17
Actions
Hour
0
500
1000
1500
2000
2500
3000
3500
0
5
10
15
20
25

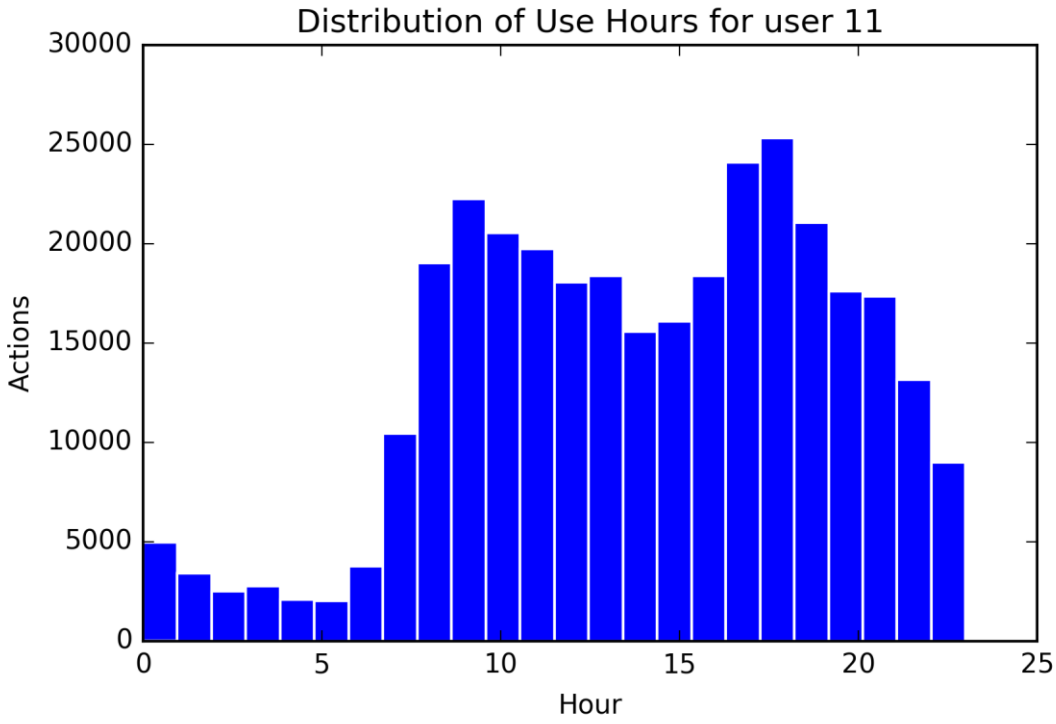

Distribution of Use Hours for user 16
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
1800
0
5
10
15
20
25

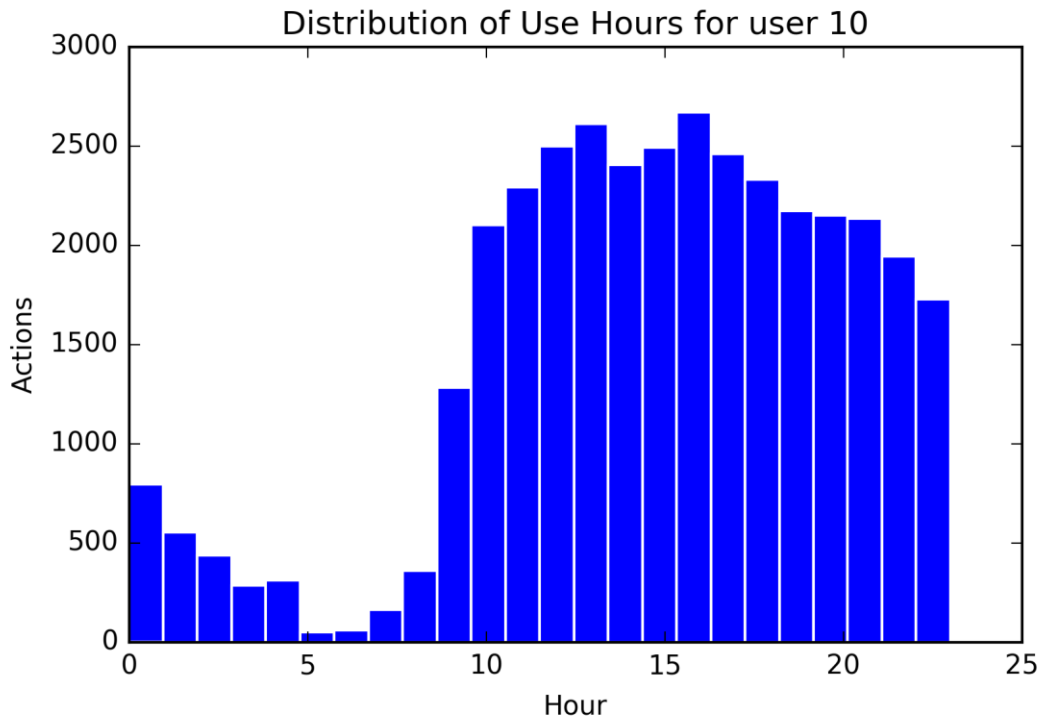

Distribution of Use Hours for user 15
Actions
Hour
0
500
1000
1500
2000
2500
0
5
10
15
20
25

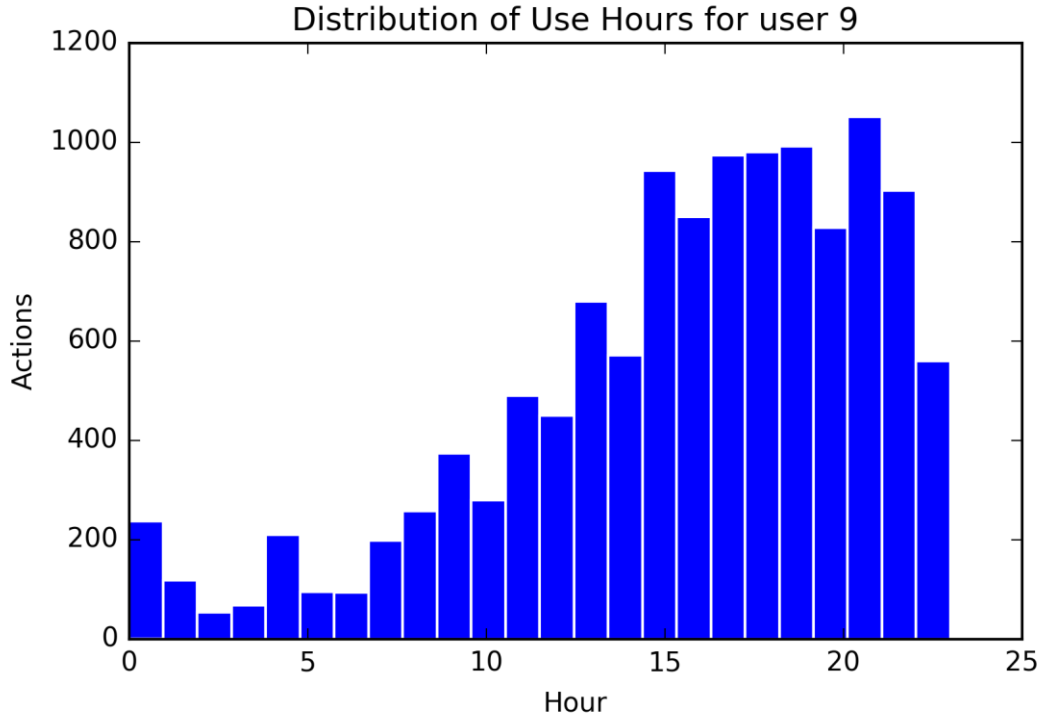

Distribution of Use Hours for user 14
Actions
Hour
0
500
1000
1500
2000
2500
0
5
10
15
20
25

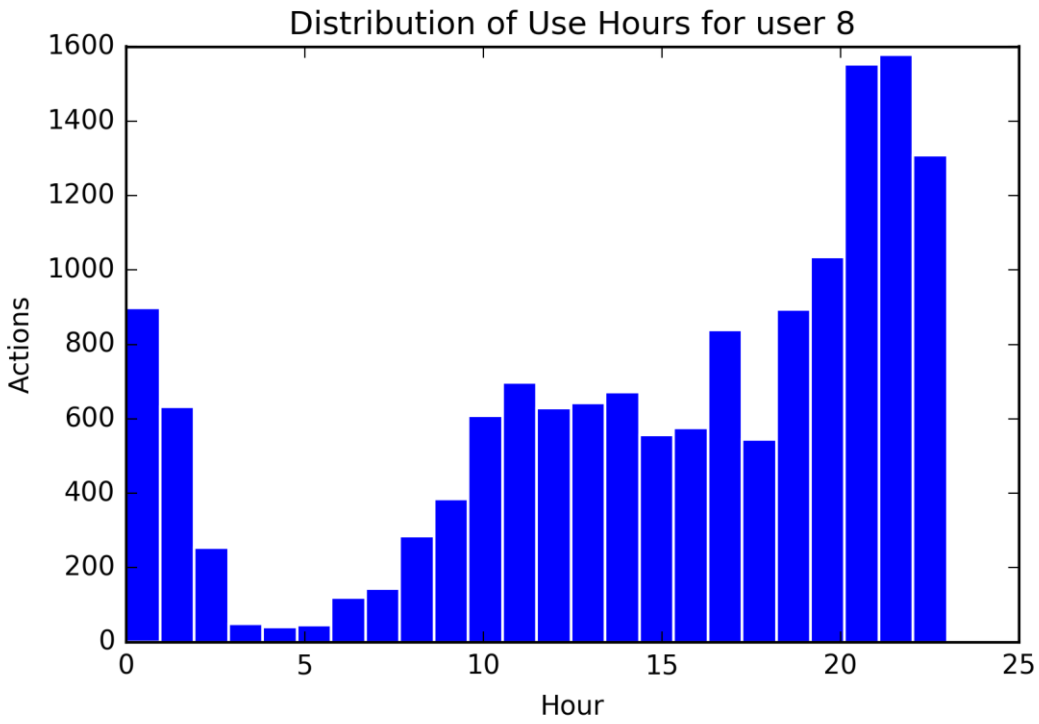

Distribution of Use Hours for user 13
Actions
Hour
0
500
1000
1500
2000
2500
3000
0
5
10
15
20
25

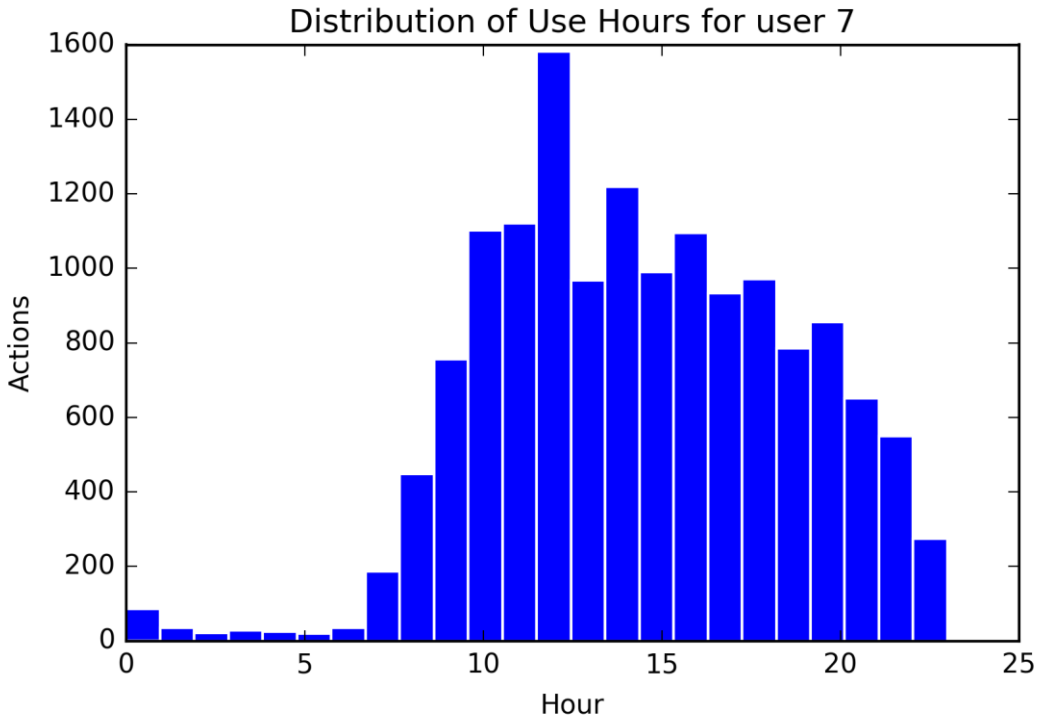

Distribution of Use Hours for user 12
Actions
Hour
0
100
200
300
400
500
600
700
0
5
10
15
20
25

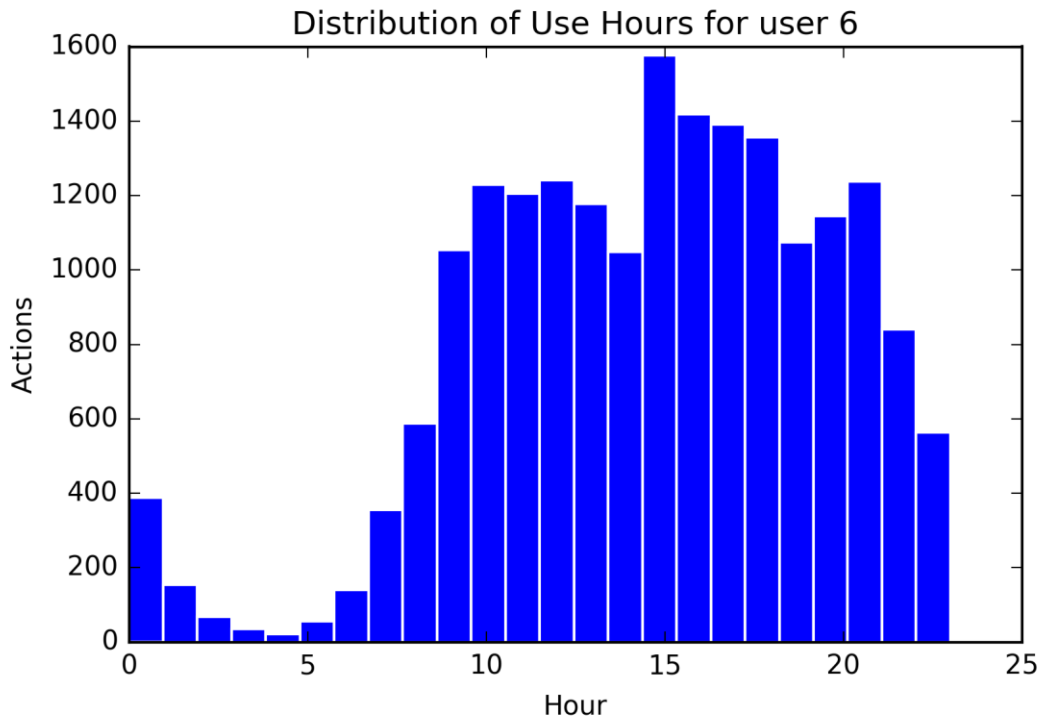

Distribution of Use Hours for user 11
Actions
Hour
0
5000
10000
15000
20000
25000
30000
0
5
10
15
20
25

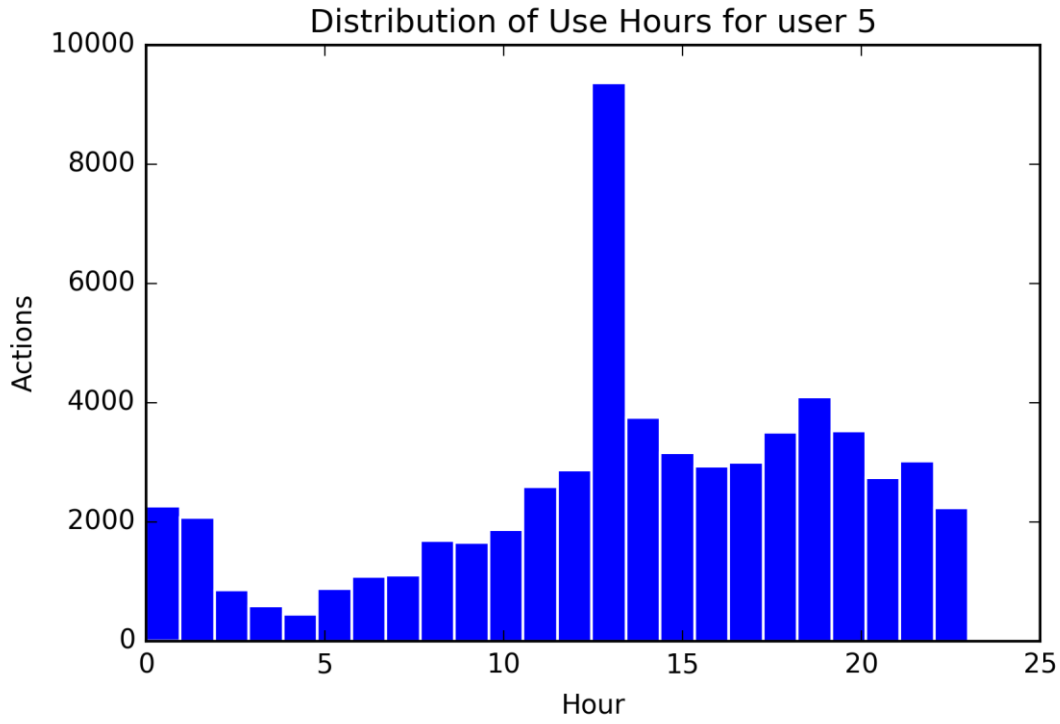

Distribution of Use Hours for user 10
Actions
Hour
0
500
1000
1500
2000
2500
3000
0
5
10
15
20
25

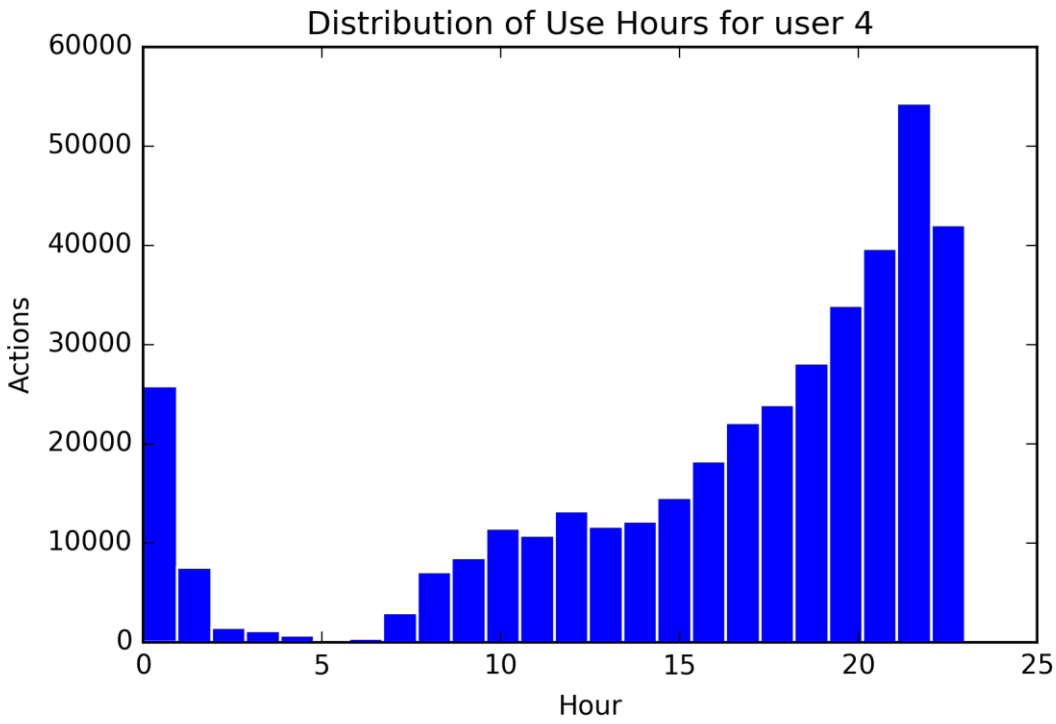

Distribution of Use Hours for user 9
Actions
Hour
0
200
400
600
800
1000
1200
0
5
10
15
20
25

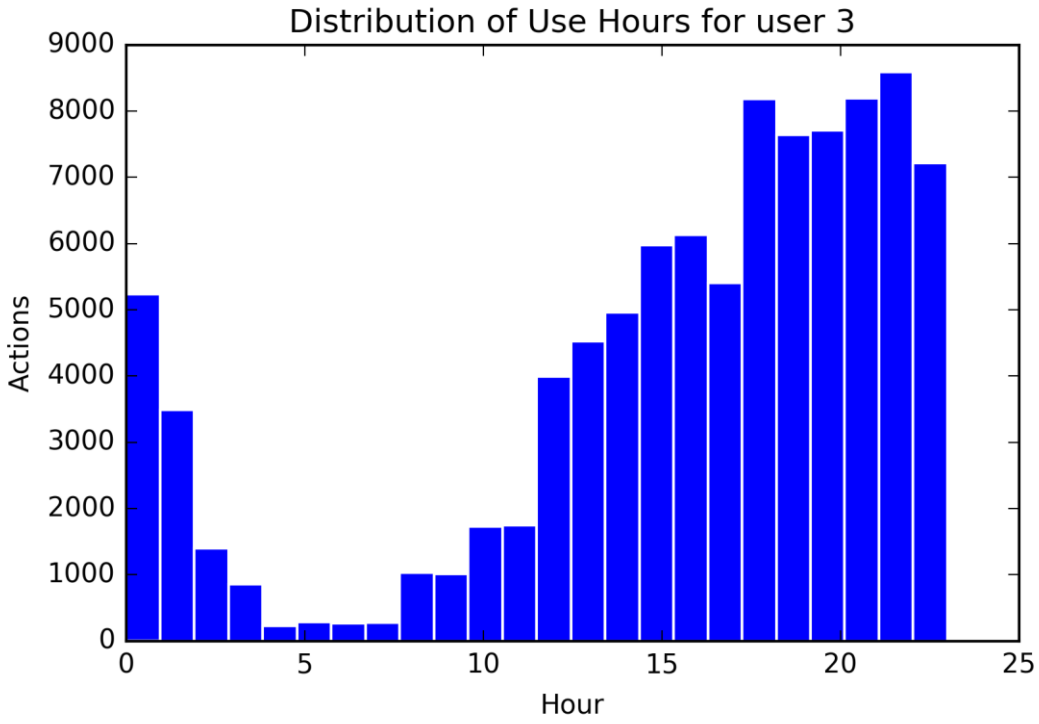

Distribution of Use Hours for user 8
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25

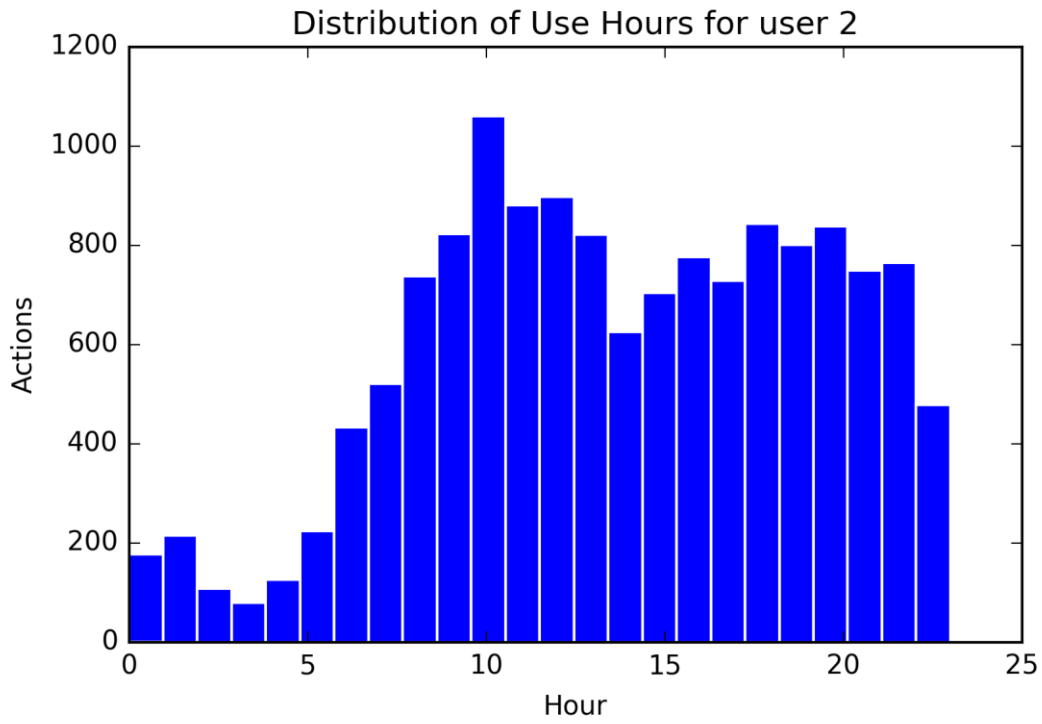

Distribution of Use Hours for user 7
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25

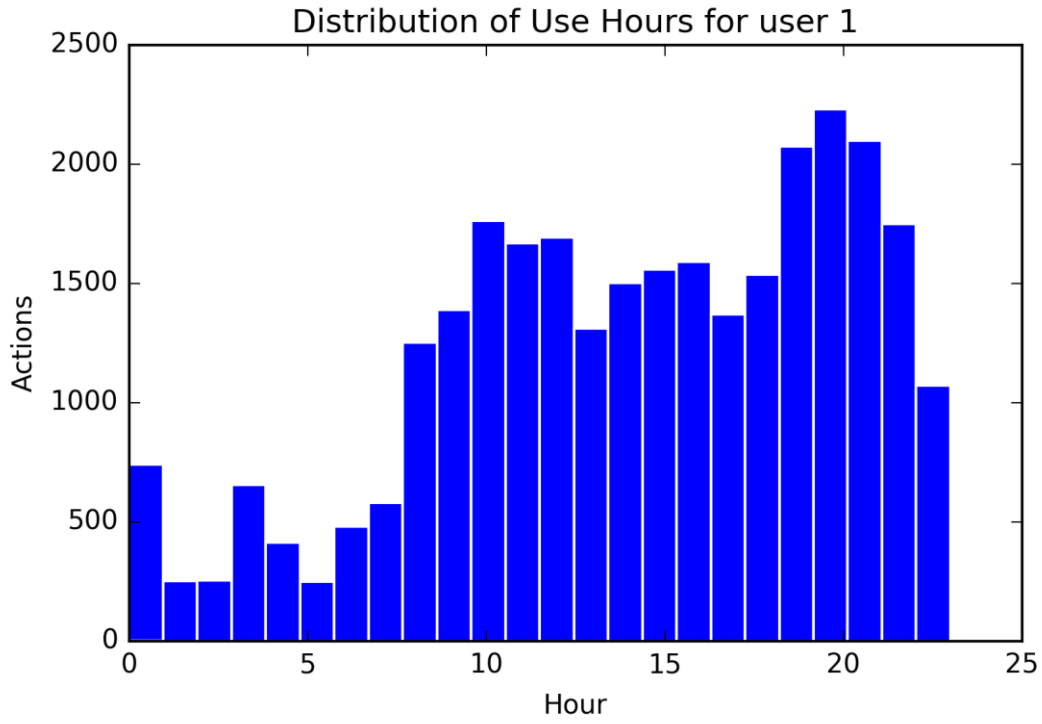

Distribution of Use Hours for user 6
Actions
Hour
0
200
400
600
800
1000
1200
1400
1600
0
5
10
15
20
25

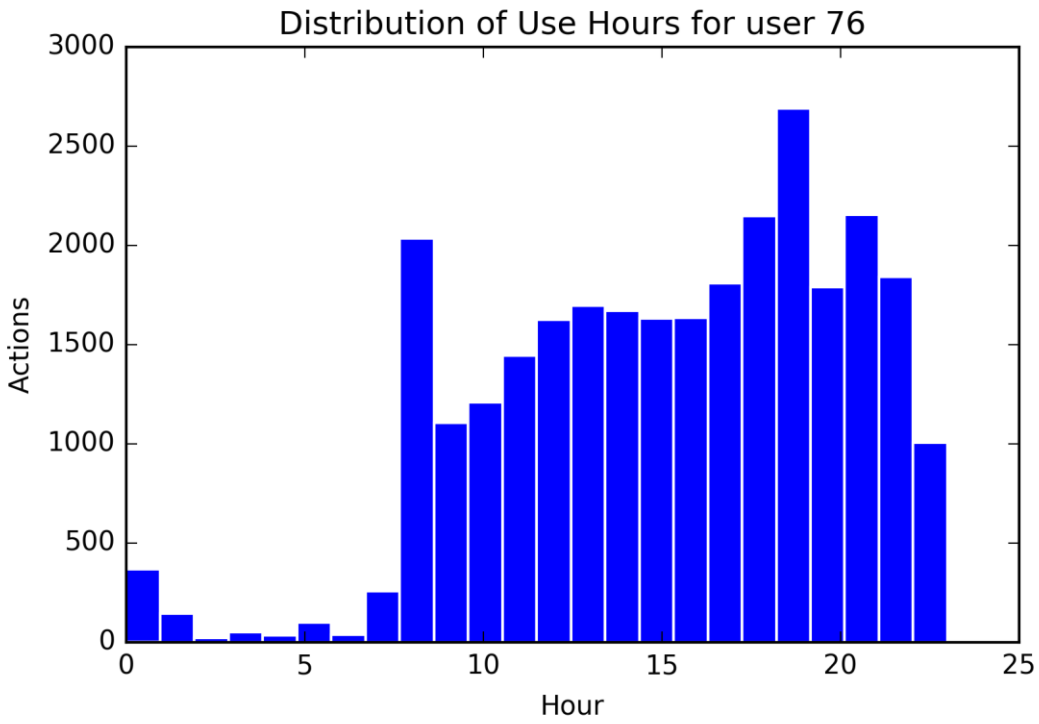

Distribution of Use Hours for user 5
Actions
Hour
0
2000
4000
6000
8000
10000
0
5
10
15
20
25

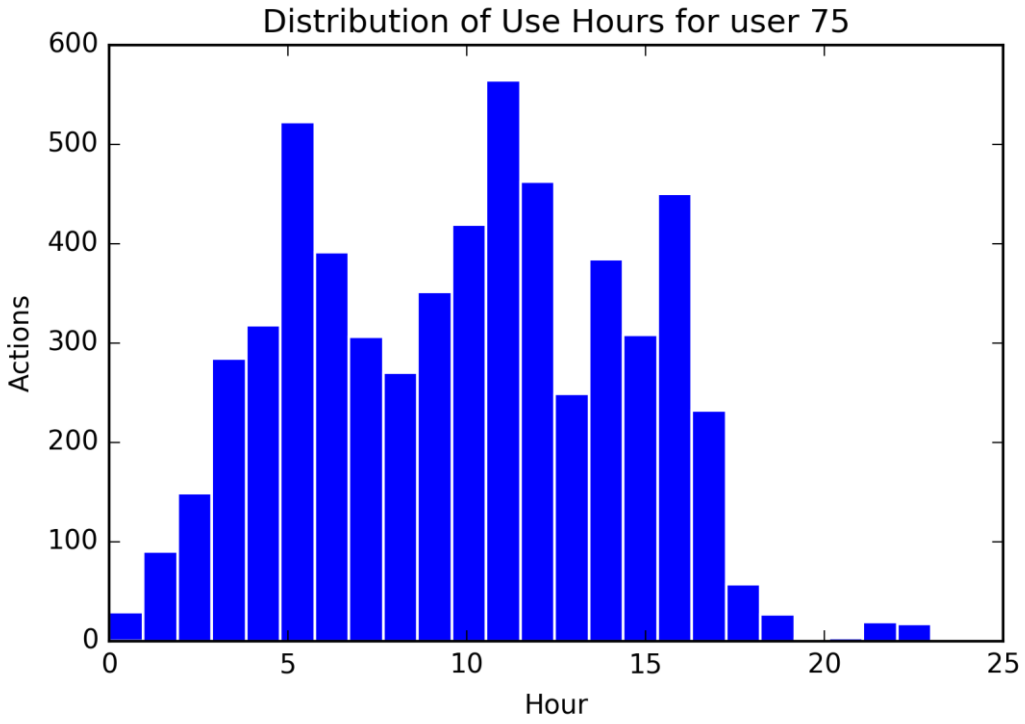

Distribution of Use Hours for user 4
Actions
Hour
0
10000
20000
30000
40000
50000
60000
0
5
10
15
20
25

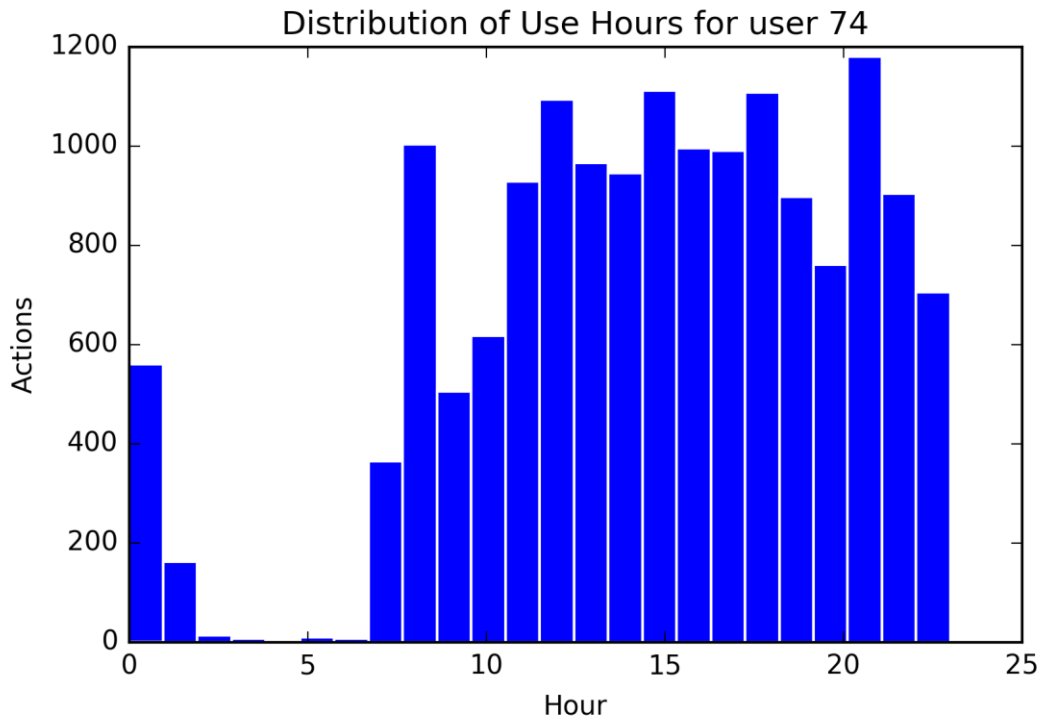

Distribution of Use Hours for user 3
Actions
Hour
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
0
5
10
15
20
25

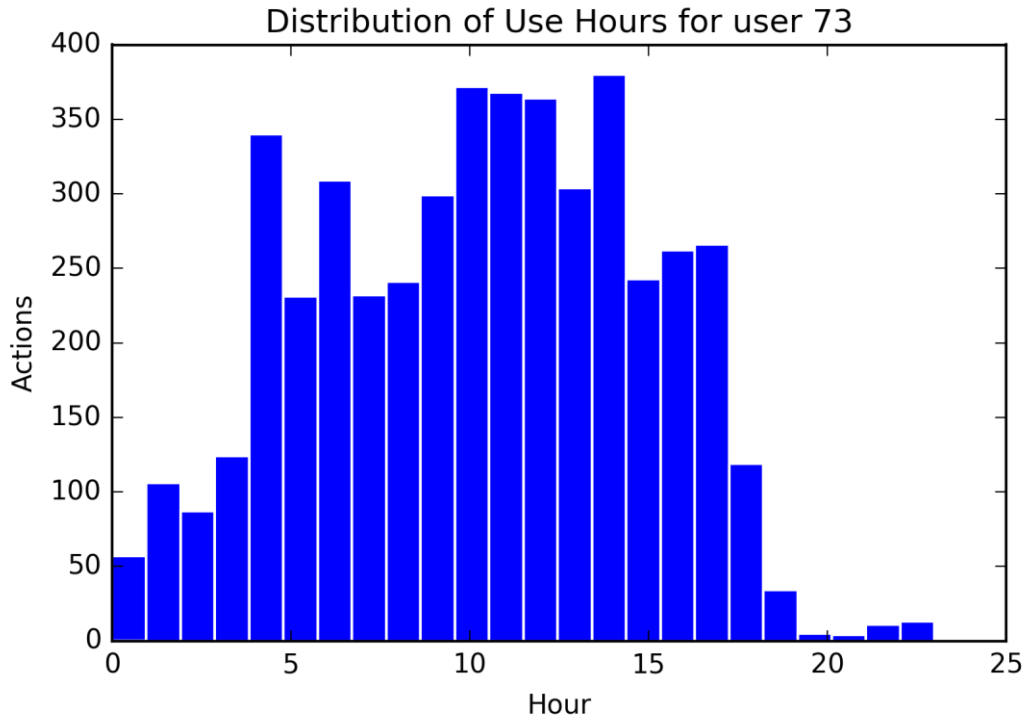

Distribution of Use Hours for user 2
Actions
Hour
0
200
400
600
800
1000
1200
0
5
10
15
20
25

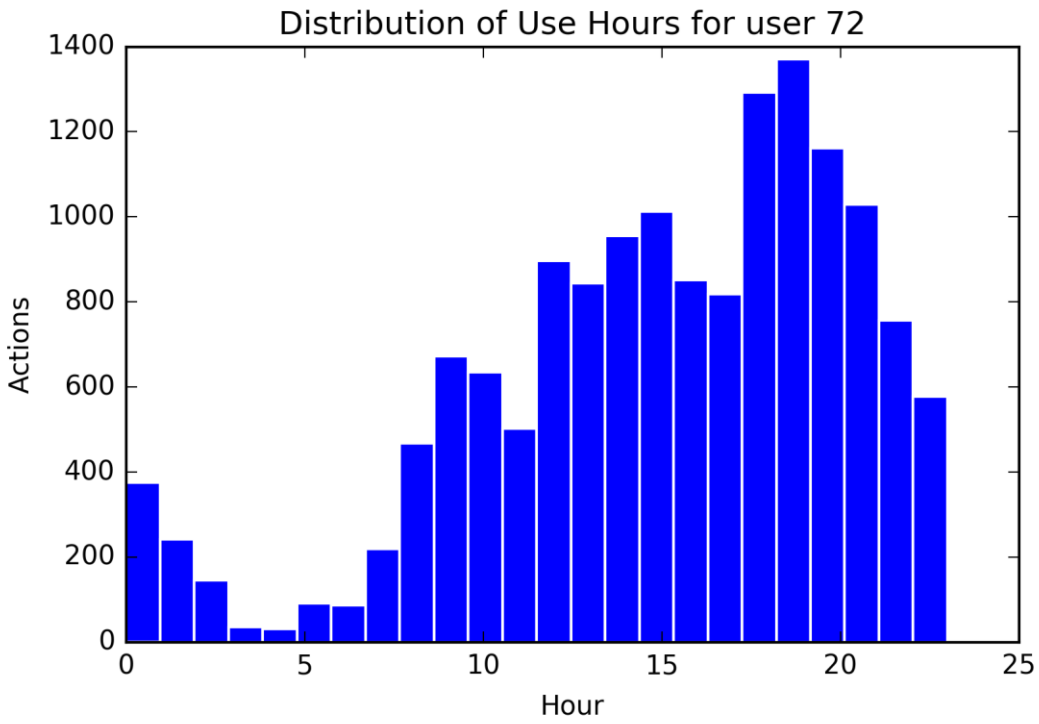

Distribution of Use Hours for user 1
Actions
Hour
0
500
1000
1500
2000
2500
0
5
10
15
20
25

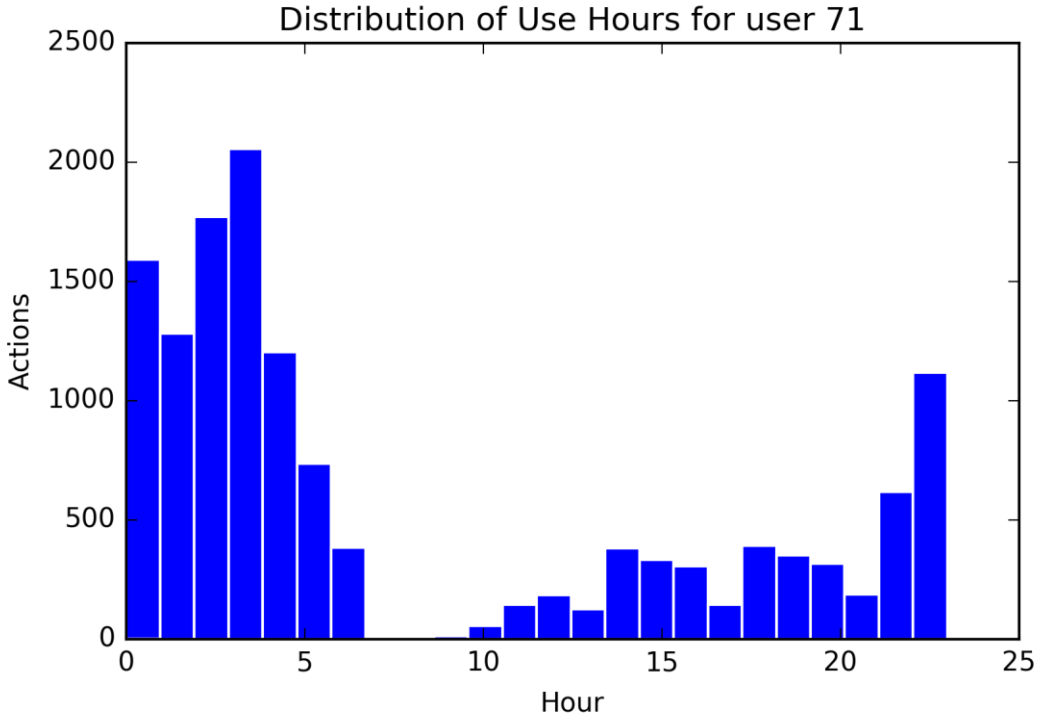

Distribution of Use Hours for user 76
Actions
Hour
0
500
1000
1500
2000
2500
3000
0
5
10
15
20
25


Distribution of Use Hours for user 75
Actions
Hour
0
100
200
300
400
500
600
0
5
10
15
20
25


Distribution of Use Hours for user 74
Actions
Hour
0
200
400
600
800
1000
1200
0
5
10
15
20
25


Distribution of Use Hours for user 73
Actions
Hour
0
50
100
150
200
250
300
350
400
0
5
10
15
20
25


Distribution of Use Hours for user 72
Actions
Hour
0
200
400
600
800
1000
1200
1400
0
5
10
15
20
25


Distribution of Use Hours for user 71
Actions
Hour
0
500
1000
1500
2000
2500
0
5
10
15
20
25